



Logius
*Ministerie van Binnenlandse Zaken en
Koninkrijksrelaties*

Diginetwerk Architectuur

Versie 0.99

Datum	15 juli 2014
Status	Finaal concept 0.99c

Colofon

Productnaam	Diginetwerk
Versienummer	
Organisatie	Logius
Bijlage(n)	0
Auteurs	Logius

Inhoud

Colofon	2
Inhoud	3
1 Inleiding	5
1.1 Doel	5
1.2 Status van dit document	5
1.3 Doel van Diginetwerk	5
1.4 Fasering in plateaus	7
1.5 Principes en Consequenties	7
1.6 Open issues in deze versie	7
2 Context en scope	8
2.1 Probleem en oplossingsrichting	8
2.2 Principes	9
2.3 Scope	10
2.3.1 Wat is Connectiviteit	10
2.3.2 Wat is een aansluiting	10
2.3.3 Voor welke connectiviteitsbehoeften	10
2.3.4 Positionering Diginetwerk en Internet	11
2.3.5 Soorten Gegevensuitwisseling	12
2.4 Beschrijving Huidige situatie	12
2.5 Streefsituatie Plateau 1	13
2.6 Toekomst: Vormen van Samenwerking	14
3 Architectuur keuzes	17
3.1 Eisen aan Diginetwerk	17
3.2 Concept Diginetwerk	18
3.2.1 Grenzen van Diginetwerk	19
3.3 Harmonisatie	19
3.3.1 IP-nummerplan en routing	19
3.3.2 DNS	24
3.4 Beveiliging	27
3.4.1 Inleiding	27
3.4.2 Compartimentering en Zones	28
3.4.3 Toepassing in Diginetwerk	28
3.4.4 Eisen/randvoorwaarden aan beveiliging tussen compartimenten/zones	30
3.5 Onderlinge koppeling van netwerken	32

3.5.1	Inleiding	32
3.5.2	Uitgangspunten koppelingen.....	33
3.6	<i>Koppelingen met BKN, type 1</i>	33
3.6.1	Eisen/randvoorwaarden BKN	34
3.6.2	Keuzes	34
3.7	<i>Koppeling Organisatie aan Diginetwerk, type 2.</i>	37
3.7.1	Inleiding	37
3.7.2	Eisen/randvoorwaarden	38
3.7.3	Partij met Diginetwerk, achter de voordeur.....	38
3.8	<i>NetworkServices</i>	39
3.8.1	Inleiding	39
3.8.2	Eisen/randvoorwaarden	40
3.8.3	Keuzes	40
3.9	<i>Grenzen van Diginetwerk in plateau 1</i>	41
3.10	<i>Beheer</i>	43
3.10.1	Inleiding.....	43
3.10.2	Architectuur en Ontwerp aspecten bij Aansluiten	44
I.	BIJLAGE I NORA Normen IB	47
II.	Bijlage DNS	49
III.	BIJLAGE Classificering uit IB-plan Logius	50
•	<i>Algemene maatregelen</i>	50

1 Inleiding

1.1 Doel

Doel van dit document

Het doel van dit document is het geven van richting aan de realisatie van Diginetwerk en het communiceerbaar documenteren van de gerealiseerde architectuur van Diginetwerk plateau 1.

Diginetwerk heette voorheen KPS (Koppelnetwerk Publieke Sector).

Doelgroep

De doelgroep wordt gevormd door architecten en technisch specialisten van alle overheidorganisaties,

1.2 Status van dit document

Dit document is finaal concept. Het is geaccordeerd door het Technisch Overleg Diginetwerk. Het wordt voorgelegd ter vaststelling door het MT van Logius.

1.3 Doel van Diginetwerk

Naar mate de eOverheid verder ontwikkeld wordt en meer gebruikt gaat worden, groeit de behoefte aan elektronische uitwisseling van verschillende aard. Daardoor ontstaat de wens om te komen tot standaardoplossingen, in dit geval voor de connectiviteit.

Het doel van Diginetwerk is om een efficiënte en effectieve standaardoplossing te bieden op het gebied van connectiviteit voor een omschreven toepassingsgebied.

Diginetwerk levert een situatie waarin elke organisatie binnen het publieke domein elke andere organisatie daarbinnen kan bereiken, op eenvoudige en gestandaardiseerde wijze via geharmoniseerde en in samenhang gekoppelde netwerken, die optimaal voorzien in de functionele connectiviteitsbehoefte.

Globale beschrijving van eisen en kenmerken

Een deel van het verkeer ook tussen overheidsorganisaties zal getransporteerd kunnen worden via internet. Echter in het geval van hoge beveiligingseisen¹ kiezen organisaties voor transport over besloten netwerken.

De afgelopen jaren heeft die behoefte aan besloten netwerkfaciliteiten geleid tot een groei van het aantal besloten netwerken en van directe verbindingen tussen overheidsorganisaties. Er zijn veel specifieke oplossingen op het gebied van connectivity ontstaan, die vaak slechts beperkt herbruikt kunnen worden. Diginetwerk zorgt voor de gewenste standaardisatie en hergebruik.

Overheidsorganisaties hebben behoefte aan een goed beveiligde, dus besloten oplossing op het gebied van connectivity, die het mogelijk maakt

¹ Beveiliging omvat Beschikbaarheid, Exclusiviteit en Integriteit.

dat ze met een eenmalige inspanning (implementatie van één stekker) gegevens – veilig en betrouwbaar – kunnen uitwisselen met alle overheidsorganisaties.

Eénmalig wil zeggen dat de eerste aansluiting aan Diginetwerk inspanning mag kosten, maar dat volgende verbindingen met andere Diginetwerk-partijen geen of nauwelijks inspanning kosten.

Het doel van Diginetwerk wordt daarmee het realiseren van een situatie m.b.t. connectiviteit, waarbij overheidsorganisaties voor verkeer met een hoger beveiligingsniveau, kunnen volstaan met één (evt redundante) aansluiting aan Diginetwerk waardoor zij connectiviteit kunnen hebben met alle andere overheidsorganisaties (die ook aan Diginetwerk zijn aangesloten). Uit standaardisatieoverwegingen wordt Diginetwerk gepositioneerd als “de” oplossing waar een besloten netwerk vereist is.

Diginetwerk waar het moet, Internet of Diginetwerk waar het kan.


De beschikbaarheid is zeer hoog (meer dan 99,9%) en Diginetwerk is volledig gescheiden van internet.

Diginetwerk is gebaseerd op hergebruik van bestaande besloten netwerken, de zog koppelnetwerken. Diginetwerk draagt ook zorg voor harmonisatie van bestaande besloten netwerken, waardoor één virtueel netwerk ontstaat. Het wordt wel een virtueel netwerk genoemd, omdat het niet een apart reëel netwerk is, maar is opgebouwd uit de verzameling van voor een groot deel bestaande en geharmoniseerde, onderling gekoppelde netwerken.

Het voordeel voor overheidsorganisaties is dat ze niet langer gebruik hoeven te maken van diverse besloten netwerken of bilaterale verbindingen, maar dat één aansluiting volstaat die voor alle eOverheid uitwisselingen kan worden herbruikt. Dat bespaart de overheidsorganisaties lijn- en beheerkosten, expertise en beheerlast.

NORA

NORA 2.0 schrijft in principe 7.3.1. voor dat communicatie tussen overheidsorganisaties besloten dient te verlopen.

<p>7.3.1</p> 	<p>Eoverheids principe</p>	<p>P17 P19</p>	<p><i>Communicatie tussen overheidsorganisaties verloopt via besloten, separate netwerken of door middel van een virtual private network verbinding via netwerken van particuliere bedrijven.</i></p>
<p>Overheid-naar-overheid communicatie verloopt bij voorkeur via private netwerken met een besloten karakter. Alternatief is het realiseren van een virtueel privaat netwerk over publieke netwerken. Het betreft in beide gevallen beslotenheid. Slechts overheidsinstanties hebben toegang tot het netwerk. Verkeer tussen overheidsinstanties kan hierdoor niet snel in handen van onbevoegde derden vallen. Bovendien is de kans op aanvallen van binnenuit in een dergelijk besloten netwerk wezenlijk kleiner dan op een openbaar netwerk.</p>			

Diginetwerk levert dat besloten netwerk.

PvU KPS

Diginetwerk is in eerste uitwerking gebaseerd op het Programma van Uitgangspunten Diginetwerk (PvU KPS) dat is opgesteld in 2006 tot 2008. Het onder dat PvU liggende concept gaat uit van een vergaande rol van telecommunicatie leveranciers. Alle organisaties hebben hun connectiviteitsvoorzieningen ingekocht bij een (of meer) telecommunicatie leveranciers. Als vervolgens alle interconnectiviteit belegd wordt bij die telecommunicatie leveranciers onderling, zouden er geen koppelnetwerken meer nodig zijn. Vooralsnog wordt dat een brug te ver geacht, en is Diginetwerk gebaseerd op het onderling koppelen van koppelnetwerken.

1.4 Fasering in plateaus

Diginetwerk wordt in plateaus gerealiseerd. Plateau 1 is bedoeld om de belangrijkste onderdelen te integreren en te harmoniseren, zodat overheidsorganisaties inderdaad met één aansluiting alle andere overheidsorganisaties (die zijn aangesloten) kunnen bereiken. De belangrijkste leidraad bij het opnemen van onderdelen in plateau 1 is de mate waarin bijgedragen wordt aan dat doel. "Optimalisaties" als bijv. dynamische routing of IPv6 maken daarom geen deel uit van plateau 1.

1.5 Principes en Consequenties

Nora en de Logius architectuurkaders onderkennen Principes. In het nieuwe NORA katern kennen principes een statement, een rationale en implicaties. Die terminologie is doorgetrokken in dit document. De hoofdbesluiten t.a.v. de Dienst Diginetwerk zijn gemarkeerd. In navolging van de NORA terminologie worden die hoofdbesluiten Implicaties genoemd, die ook als statement zijn geformuleerd.

1.6 Open issues in deze versie

Een aantal zaken zijn nog niet in deze versie van de architectuur en in plateau 1 opgenomen. Het betreft zaken die (mogelijk) wel gewenst zijn in toekomstige versies.

- Een centrale/gemeenschappelijke toegang tot internet.
- Duidelijk gedefinieerde QoS (en monitoring daarop) en het opnemen van CoS
- DNS Reverse lookup
- Uitwerking van transparantie van Diginetwerk (alles helemaal open of niet)
- Optimale wijze van aansluiting van bedrijfsnetwerken/rekencentra (en internet) aan Diginetwerk (evt. als "best practises" bijlage)

2 Context en scope

2.1 **Probleem en oplossingsrichting**

De groeiende realisatie van de eOverheid vereist dat er steeds meer informatie uitgewisseld wordt tussen organisaties met een publieke taak (publiek en privaat), burgers en medewerkers van organisaties. Dit is vastgelegd in verschillende beleidsnotities en architectuur documenten². De consequentie van die uitgebreidere uitwisseling, nl de behoefte aan meer standaardisatie en betere koppelingsvoorzieningen zijn bijv. in het NUP onderkend.

In het NUP is in paragraaf 4.3 gesteld:

De OSB veronderstelt dat de verschillende overheidsnetwerken aan elkaar gekoppeld zijn. Dat impliceert aansluiting op de Haagse Ring en gebruik van de standaarden van het Koppelnets Publieke Sector.

Hoewel gebruik van internet in veel gevallen een adequate oplossing biedt, zijn voor veel overheidsorganisaties besloten netwerkoplossingen gewenst of noodzakelijk (zie ook par. 3.4).

Er is daardoor een steeds grotere behoefte aan standaardoplossingen voor connectiviteit. Zonder dergelijke standaardoplossingen zijn publieke organisaties gedwongen om ieder voor zich telkens opnieuw connectiviteitsoplossingen te bedenken en te realiseren. Daardoor is er een veelheid aan datalijnen en technische oplossingen ontstaan.

Organisaties hebben thans diverse verschillende lijnen van diverse telecommunicatie leveranciers ingekocht en in gebruik. Zowel de kosten van die lijnen als de beheerkosten in de meest brede zin zijn daarom veel hoger dan noodzakelijk, en aanleg van nieuwe verbindingen kost veel tijd.

De oplossing van dit probleem ligt in het bieden van een stelsel van afspraken en voorzieningen, dat het mogelijk maakt dat organisaties nog maar één aansluiting nodig hebben om op een standaard manier met elkaar te kunnen communiceren, d.w.z. connectiviteit te kunnen hebben met alle andere organisaties in het publieke domein.

² [NORA], [MARIJ], [GEMMA] [NUP], etc

2.2

Principes

De voor Diginetwerk relevante Principes uit NORA zijn hieronder opgesomd. Diginetwerk is een infrastructuur dienst die vooralsnog uitsluitend geboden wordt aan Overheidsorganisaties en niet aan Burgers en Bedrijven. Een groot deel van de NORA principes is daardoor niet/nauwelijks van toepassing. Alleen de van toepassing zijnde principes zijn hieronder (verkort) opgenomen.

AP 5	Gebruik standaard oplossingen	<i>De dienst maakt gebruik van standaard oplossingen</i>
	Afgeleid	Standaard: "Afnemers ervaren uniformiteit in de dienstverlening door het gebruik van standaardoplossingen."
AP 7	Gebruik open standaarden	Statement <i>De dienst maakt gebruik van open standaarden</i>
AP 27	Afspraken vastgelegd	Statement <i>Dienstverlener en afnemer hebben afspraken vastgelegd over de levering van de dienst</i>
AP 28	Consequenties van normafwijking	Statement <i>Wanneer wordt afgeweken van afspraken en standaarden draagt de dienstverlener zelf de consequenties daarvan.</i>
		Implicaties Alle partijen moeten zich aanpassen c.q. rekening houden met de gevestigde communicatienormen en -standaarden. Partijen die zich niet conformeren, lopen de kans uitgesloten te worden om een bijdrage te leveren aan de dienstverlening.
AP 29	Verantwoording dienstlevering mogelijk	Statement <i>De wijze waarop een dienst geleverd is, kan worden verantwoord</i>
AP 32	Baseline kwaliteit diensten	Statement <i>De dienst voldoet aan de kwaliteitsbaseline</i>
		Afgeleid <input type="checkbox"/> Standaard: "Overeenkomstige aspecten van dienstverlening krijgen op overeenkomstige wijze vorm door gebruik te maken van generieke oplossingen die breed worden toegepast". <input type="checkbox"/> Betrouwbaar: "De beschikbaarheid en de kwaliteit van diensten voldoen aan vooraf bepaalde normen".
AP 33	Verantwoording kwaliteit	Statement <i>De dienstverlener legt verantwoording af over de besturing van de kwaliteit van de dienst.</i>
		Afgeleid <input type="checkbox"/> Transparant: "Afnemer hebben inzage in voor hen relevante informatie" <input type="checkbox"/> Betrouwbaar: "de beschikbaarheid en de kwaliteit van diensten voldoen aan vooraf

		bepaalde normen”.
AP 34	Continuïteit van de dienst	Statement <i>De levering van de dienst aan de afnemer is continu gewaarborgd.</i>
		Afgeleid Betrouwbaar: “De beschikbaarheid en de kwaliteit van diensten voldoen aan vooraf bepaalde normen.”
AP 37	Informatiebeveiliging door zonering en filtering	Statement <i>De betrokken faciliteiten zijn met behulp van filters gescheiden in zones</i>

2.3 Scope

Diginetwerk is niet bedoeld om een antwoord te zijn op alle denkbare vormen van connectiviteit. Het richt zich op die beveiligde connectiviteitsbehoeften die voortvloeien uit de eOverheid. Welke vormen binnen scope vallen wordt hieronder toegelicht.

2.3.1 Wat is Connectiviteit

Onder connectiviteit wordt verstaan de aansluitbaarheid van verschillende computersystemen van diverse leveranciers via telecommunicatienetwerken, resp. het gemak waarmee dat kan. In zijn algemeenheid vereist het onderling communiceren (op elkaar aansluiten) van computersystemen een veelheid van interoperabele afspraken resp. standaarden. Deze standaarden worden gebruikelijk ondergebracht in een lagen model, bijv. het ISO-OSI model, of - in de wereld van internetstandaarden - de TCP/IP stack.

Diginetwerk richt zich op de onderste drie lagen van het OSI model ³, de basisconnectiviteit.
Hogere lagen worden ingevuld door bijv. Digikoppeling-standaarden en daarboven diverse semantische en organisatorische interoperabiliteits-standaarden.

De onderste 3 lagen zijn:
-Physical layer (bijv. RJ45 stekker)
-Data Link layer (bijv. ethernet)
-Network layer (IP)

2.3.2 Wat is een aansluiting

Een aansluiting aan Diginetwerk bestaat uit een laag 3 dienst (zie paragraaf 3.5) gecombineerd met aansluitvoorwaarden geleverd door een koppelnetwerkbeheerder.

2.3.3 Voor welke connectiviteitsbehoeften

Organisaties hebben behoefte aan diverse soorten elektronische samenwerking.

³ overeenkomend met de onderste drie lagen van de five layer TCP/IP model

1. Soms is er behoefte aan samenwerking tussen autonome overheidsorganisaties,
2. soms dient de samenwerking tussen medewerkers (ambtenaren) van verschillende organisaties geïntensiveerd te worden en wordt gekeken naar de aspecten: locatie, tijdstip, toepassingen en werkwijze,
3. soms gaat het om elektronische communicatie tussen overheidsorganisaties en burgers, resp. bedrijfsleven.

Zo zijn nog diverse andere soorten te onderscheiden.

Keuze voor Plateau 1

Binnen al die mogelijkheden is voor Diginetwerk in plateau 1 primair de connectiviteit t.b.v. uitwisseling tussen overheidsorganisaties (punt 1) over een besloten netwerk van belang. Hieronder wordt verstaan zowel de uitwisseling tussen systemen van overheidsorganisaties onderling (S2S) als tussen medewerkers (met een browser) van de ene organisatie en systemen (website) van een andere organisatie (P2S).

Diginetwerk levert de noodzakelijke connectiviteit t.b.v. elektronische samenwerking van overheidsorganisaties en hun medewerkers.

Voor een volgend plateau kan deze keuze worden heroverwogen, zie ook paragraaf 2.6.

Private Organisaties met een publieke taak worden vooralsnog niet als een primaire doelgroep voor Diginetwerk beschouwd.

2.3.4

Positionering Diginetwerk en Internet

Diginetwerk faciliteert de uitwisseling tussen overheidsorganisaties. De informatie die uitgewisseld wordt is bepalend voor het niveau van de beveiligingseisen die gesteld worden (rubricering). Omdat informatie-uitwisseling binnen ketens plaatsvindt horen de beveiligingseisen bij ketens, voor bepaalde informatiestromen. De keten waarin bijvoorbeeld GEO (BAG) gegevens worden uitgewisseld zal lagere beveiligingseisen (t.a.v. exclusiviteit) stellen dan bijv. de GBA-keten, de zorgketen, de OOV-keten etc.. Overigens kunnen eisen aan beschikbaarheid bij bijv. de GEO gegevens wel weer hoger zijn dan bij andere ketens en gegevens. De eisen aan de betrouwbaarheid van de voorziening Diginetwerk worden bepaald door de afhankelijkheid van organisaties van die voorziening. Het niveau van betrouwbaarheid (Beschikbaarheid, Exclusiviteit en integriteit) wordt wel classificatie genoemd.

Er zijn ketens waarin een besloten netwerk (al of niet expliciet zoals bij GBA) gezien de rubricering van de gegevens en/of de classificatie van de betrouwbaarheid vereist is. Alle uitwisselingen m.b.t. die keten moeten dus via een besloten netwerk, lees Diginetwerk. Andere ketens hebben mogelijk lagere eisen en mogen via internet.

Vrijwel allen overheidspartijen zullen zitten in een of meer ketens die hoog beveiligd zijn (bijv GBA-keten). Ze moeten dus allemaal een aansluiting

hebben aan Diginetwerk. Als er vervolgens gekozen zou worden om een andere keten met lagere beveiligingseisen (waarbij meestal dezelfde partijen betrokken zijn) via internet te laten lopen, dan is daar vanuit beveiligingsoptiek in principe niets tegen. Organisaties kunnen wel kiezen om toch het verkeer via Diginetwerk te laten lopen, bijvoorbeeld vanuit standaardisatie optiek.

Diginetwerk is bedoeld voor uitwisselingen tussen overheidsorganisaties waarvoor een hoog niveau van betrouwbaarheid/beveiliging vereist is.

Dit is nader uitgewerkt in paragraaf 3.4.

2.3.5

Soorten Gegevensuitwisseling

Diginetwerk is bedoeld voor het verzorgen van de connectiviteit die nodig is bij de verschillende soorten gegevensuitwisseling tussen overheidspartijen.

Voor samenwerkende organisaties worden de volgende soorten uitwisseling onderkend:

1. Digikoppeling (OSB) verkeer. Dat is zg. berichtenverkeer, system-to-system, gebaseerd op de Digikoppeling-standaarden, d.w.z. SOAP over HTTPs. Andere vormen van System-to-system die ook gebaseerd zijn op HTTP(s), maar die (nog) niet voldoen aan Digikoppeling standaarden kunnen hier ook onder gerekend worden.
2. websiteverkeer. Dat is het verkeer tussen een browser op een werkplek en een website/portal. Dat verkeer is gebaseerd op HTTPs en HTTP.
3. Mail. Dat is het verkeer waarmee emails worden uitgewisseld; wordt uitgewisseld tussen mailservers, op basis van SMTP.
4. Filetransfer. Hiermee worden bestanden uitgewisseld op basis van FTP of FTPs.

Prioriteit ligt bij de typen 1 en 2, d.w.z. HTTP en HTTPs verkeer. Consequenties van mailverkeer (welke maildiensten moeten zijn ingericht in de betrokken koppelnetwerken) en van Filetransfer (wat is impact op capaciteit) moeten eerst onderzocht worden voordat deze verkeerssoorten worden toegelaten.

Diginetwerk richt zich primair op de ondersteuning van HTTPS en HTTP verkeer.

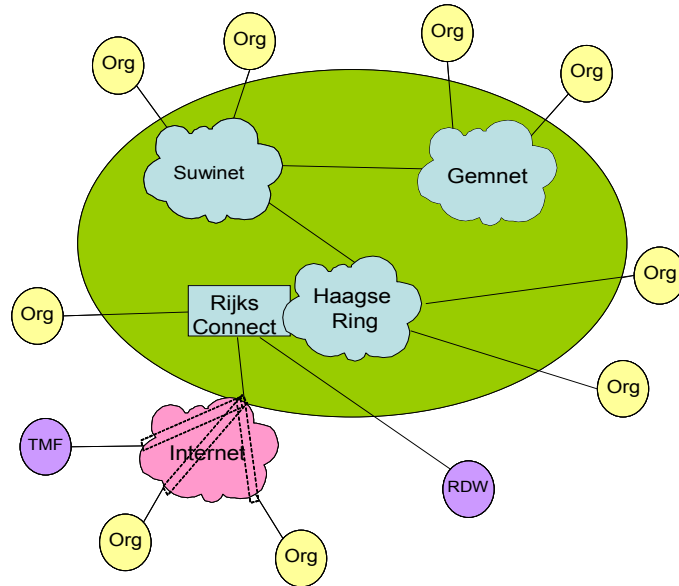
Vooralsnog wordt geen rekening gehouden met verkeerssoorten als VoIP, streaming video of audio etc.

2.4

Beschrijving Huidige situatie

Diginetwerk bouwt voort op de Haagse Ring en andere resultaten van het voormalige ICTU-project Bundeling Landelijke Netwerken (BLN).

Dat heeft per medio 2009 geleid tot onderstaande situatie :



Figuur 1 Situatie per medio 2009

In deze situatie kunnen al een aantal verbindingen op dezelfde manier gebruikt worden, resp. hergebruikt voor andere informatiestromen, maar het is niet de beoogde eindsituatie. Er is nog geen sprake van harmonisatie.

2.5

Streefsituatie Plateau 1

In de streefsituatie medio 2010 dienen de in het kader van het NUP belangrijkste koppelnetwerken onderling gekoppeld te zijn, zodat een organisatie die aangesloten is aan een van de koppelnetwerken – onder bepaalde beveiligingsvoorwaarden - zonder aanpassingen gebruik kan maken van services van andere overheidsorganisaties aangesloten aan hetzelfde of aan andere koppelnetwerken.

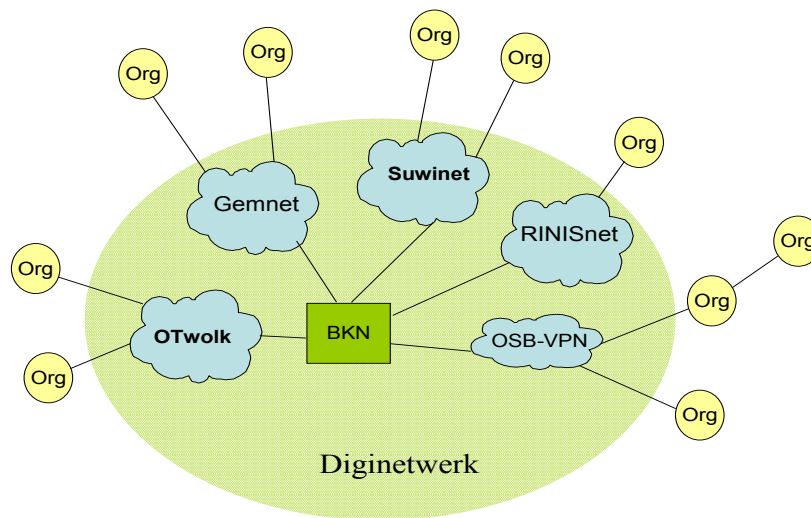
Anders gezegd: Diginetwerk plateau 1 zorgt dat een overheidsorganisatie connectiviteit heeft met alle andere overheidsorganisaties die zijn verbonden met die koppelnetwerken vallend binnen de grenzen van Diginetwerk.

In plateau 1, medio 2010, zijn relevante koppelnetwerken:

- VPN's op Haagse Ring
- Gemnet
- Suwinet
- Een nieuw in te richten koppelnetwerk, met als werknaam de OT-wolk.
- RINISnet

De koppelnetwerken zijn onderling gekoppeld via het Basis Koppel Netwerk BKN.

De diverse Overheidsorganisaties (in de figuur aangeduid met Org) zijn aangesloten aan een koppelnetwerk, en omdat de koppelnetwerken onderling zijn verbonden kan iedere "Org" communiceren met iedere andere "Org" (mits toegestaan).
In de navolgende tekst wordt "Org" gebruikt om een aan Diginetwerk aangesloten organisatie aan te duiden.



Figuur 2 Diginetwerk Plateau 1

Dit is te beschouwen als de eerste concrete invulling van Diginetwerk. De architectuur van Diginetwerk, als beschreven in hoofdstuk 3, houdt natuurlijk rekening met die eerste invulling, maar abstraheert wel om een ook op langere termijn stabiele architectuur te kunnen neerzetten.

2.6 Toekomst: Vormen van Samenwerking

Deze paragraaf gaat nader in op het hierboven in paragraaf 2.3.5 genoemde verschil tussen "samenwerking tussen overheidsorganisaties" en "samenwerking tussen ambtenaren". Voor plateau 1 is gekozen voor alleen ondersteuning van samenwerking tussen overheidsorganisaties. Later kan dat uitgebreid worden.

Zowel elektronisch samenwerkende overheidsorganisaties als elektronisch samenwerkende ambtenaren hebben behoefte aan connectiviteit. De eisen, benodigde voorzieningen en verantwoordelijkheden zijn echter gedeeltelijk verschillend.

In deze paragraaf worden beide doelgroepen en hun eisen en wensen nader uitgewerkt, met als doel op termijn te komen tot één visie op en architectuur van de gezamenlijke onderliggende laag connectiviteit.

Samenwerking tussen organisaties

Veel bedrijfstoepassingen worden gevoed met informatie vanuit andere organisaties, werken daar mee samen of worden in het geheel door andere dan de eigen organisatie aangeboden.

Dit alles vereist connectiviteit tussen de organisaties binnen de publieke sector en connectiviteit vereist op zijn beurt het koppelen en toegankelijk maken van reeds bestaande netwerken. Zie de navolgende impressie.

Bij samenwerkende organisaties is sprake van bedrijfssystemen die onderling gekoppeld zijn en berichten resp. informatie uitwisselen (in termen van SOA: gebruik maken van elkaars services, zie NORA), ofwel bedrijfssystemen die ook (deels) beschikbaar gesteld worden aan medewerkers van andere organisaties (webapplicaties).

De samenwerkende organisaties hebben via gedefinieerde uitwisselingskanalen (met een beperkt aantal protocollen) contact met elkaar, waarbij ieder zijn eigen verantwoordelijkheden en autonomie behoudt. Ze zijn Loosely Coupled, conform het concept van (web)services. Diginetwerk is echter niet alleen bedoeld voor berichtenverkeer op basis van webservices zoals gestandaardiseerd in Digikoppeling (voorheen OSB). Ook email-verkeer (SMTP) en filetransfer (FTP) tussen overheidsorganisaties (dus via besloten netwerk) behoort tot de doelprotocollen.

Samenwerkende (rijks)ambtenaar

Vanaf de werkplek kan, waar deze zich ook bevindt of hoe deze eruitziet, een aantal toepassingen worden gestart. Denk hierbij aan toepassingen ter ondersteuning van het primaire proces, HRM toepassingen, nieuws en informatie toepassingen, samenwerkingstoepassingen, toepassingen voor het afhandelen van privé aangelegenheden, etc. De nieuwe generatie ambtenaren zal daarnaast ook nog eens sterker leunen op online voorzieningen zoals zoekdiensten, chat, sms, social networking, etc.

Samenwerkende ambtenaren willen hun omgeving ervaren alsof ze samen op één LAN zitten met alle daarbij behorende kantoorautomatiserings-faciliteiten en protocollen. Het samenwerkingsverband is relatief open voor wie zich daarbinnen bevindt. Ze zijn Tightly Coupled.

Er moeten allerlei voorzieningen ingericht worden om organisaties te laten samenwerken, en ook om de samenwerkende (Rijks)ambtenaar te ondersteunen. Dat laatste is het aandachtsgebied van Digitale Werkomgeving Rijksdienst (DWR).

Gewenst is dat op termijn beide samenwerkingsvormen gebruik maken van dezelfde onderliggende connectiviteitslaag. Die gezamenlijke connectiviteitslaag zou dan verzorgd moeten worden door Diginetwerk. Vooralsnog wordt de samenwerking rijksambtenaar alleen ondersteund op de Haagse Ring omgeving binnen DWR. Het valt daarom vooralsnog buiten de scope van Diginetwerk.

Algemeen

Belangrijk hierbij is dat het niet sec gaat om de netwerken of het koppelen daarvan, maar om het kunnen voorzien in de benodigde functionaliteit (nu en in de toekomst). De in samenhang gekoppelde netwerken dienen zich daarom te gedragen als een geïntegreerde oplossing en bouwsteen (dienst), waarmee de benodigde functionaliteit kan worden gerealiseerd.

Dit wordt bereikt door netwerken niet alleen te koppelen, maar deze tevens te harmoniseren.

3 Architectuur keuzes

3.1 Eisen aan Diginetwerk

De hoofdeisen die gesteld worden aan Diginetwerk liggen op het gebied van:

- Beveiliging; Diginetwerk moet als besloten netwerk voldoen aan de hoge beschikbaarheids- en exclusiviteits- en integriteitseisen, die voor Organisaties reden zijn om voor Diginetwerk te kiezen; het gaat hier om de eisen gesteld aan gegevensstromen (rubricering) en om de eisen gesteld aan de voorziening Diginetwerk, bezien vanuit de afhankelijkheid van Organisaties van Diginetwerk (classificatie).
- Eenvoud van aansluiting; Organisaties moeten eenmalig aansluiten aan Diginetwerk en vervolgens zonder aanpassingen op het gebied van connectiviteit kunnen communiceren met (services van) andere Organisaties.
- Transparantie en openheid; Diginetwerk is voor de aangesloten partijen zo transparant mogelijk, d.w.z. geen adresvertalingen en geen firewalls (tenzij noodzakelijk vanuit beveiliging)
- Beheer; betreft met name wijzigings-, incident-, servicelevel- en capaciteitsmanagement. De architectuur dient zodanig te zijn dat bijvoorbeeld nieuwe aansluitingen en onderlinge koppelingen met minimale inspanning gerealiseerd kunnen worden.
- Open Standaarden. Het gebruik van open standaarden spreekt uiteraard vanzelf. Een voorziening als Diginetwerk die maximale interoperabiliteit als kernfunctie heeft, kan uitsluitend functioneren op basis van open standaarden.
- Hergebruik van bestaande voorzieningen resp. reeds in het verleden gedane investeringen.
- Kwaliteit (QoS); dit betreft zowel zaken als latency etc, maar ook eventueel het differentiëren naar Classes of Service.

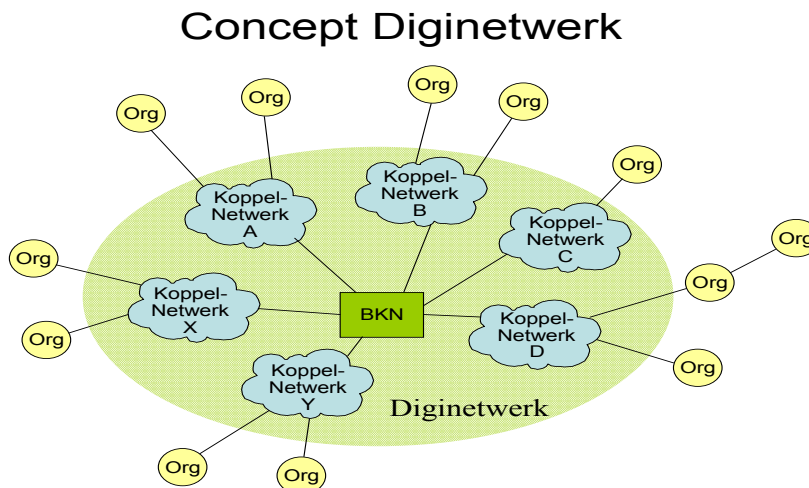
Deze eisen hebben geleid tot een concept van Diginetwerk, dat hierna wordt geschetst. Vervolgens zal worden ingegaan op de diverse onderdelen van het eisenpakket. Er zit een zekere overlap tussen eisen en bijbehorende architectuurkeuzes. Sommige keuzes vormen een invulling van meerdere eisen, bepaalde keuzes houden ook een – vaak pragmatische – keuze voor een optimum in.

In plateau 1 zal nog niet aan alle wensen voldaan worden. Van diverse wensen is aangegeven dat die in plateau 1 vooralsnog niet zijn meegenomen, en dus in een volgend plateau moeten komen.

3.2

Concept Diginetwerk.

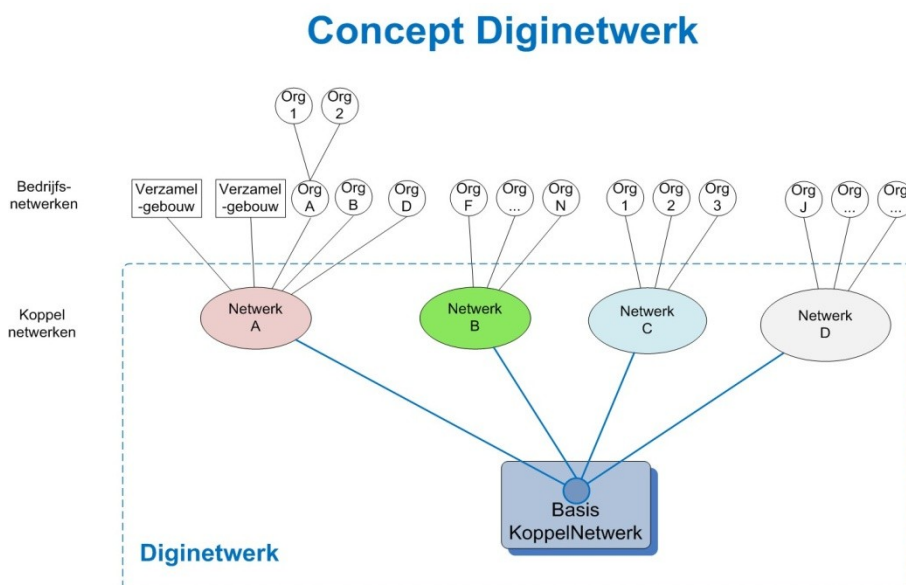
Het concept van Diginetwerk is geschetst in onderstaande figuur.



Figuur 3 Praatplaat Concept Diginetwerk

Diginetwerk is opgebouwd uit diverse koppelnetwerken, die onderling geharmoniseerd en gekoppeld zijn. Organisaties zijn – in principe – aangesloten op één koppelnetwerk (zie ook par. 3.7). De onderlinge koppeling gebeurt in het BasisKoppelNetwerk BKN.

Bovenstaande Figuur 2, de “praatplaat” heeft voordelen bij breed georiënteerde communicatie. Voor dit architectuurdocument wordt onderstaande figuur gehanteerd als basis voor de verdere uitwerking.



Figuur 4 Basisarchitectuur Diginetwerk

In de volgende paragrafen zal deze basisarchitectuur nader uitgewerkt worden, vanuit diverse aspecten bezien. Gezien de relatie tussen de verschillende aspecten zullen bepaalde onderwerpen bij diverse aspecten terugkomen. De behandelde aspecten zijn:

- Harmonisatie; dit betreft Diginetwerk-brede zaken als IP-nummerplan, routing, DNS-resolving,
- Compartimenten en beveiliging
- Onderlinge koppelingen
- Netwerkservices
- Beheer

Aangezien veel van deze onderwerpen een sterke onderlinge relatie hebben, is een strikt gescheiden behandeling per onderwerp lastig. Er moet dan immers vaak verwezen worden naar onderwerpen die verderop behandeld worden. In deze versie van dit document is daar toch voor gekozen.

3.2.1 *Grenzen van Diginetwerk*

Diginetwerk bestaat onder andere uit een verzameling koppelnetswerken. Binnen de hele overheid bestaan veel meer koppelnetswerken dan die nu opgenomen zijn in Diginetwerk. Het is daarom nodig om te bepalen welke koppelnetswerken behoren tot Diginetwerk en welke niet.

Koppelnetswerken behoren tot Diginetwerk, wanneer ze voldoen aan het stelsel van Diginetwerk-afspraken en dus ook aan eisen aan Diginetwerk, zoals eenvoud van aansluiting en transparantie.

Koppelnetswerken buiten de grenzen van Diginetwerk zijn dus per definitie "anders" dan die er binnen; ze kennen op onderdelen andere IP-nummerplannen, andere beveiligingsregimes, andere procedures etc.. Overigens kunnen uiteraard bepaalde eigenschappen en procedures wel gelijk zijn, bijvoorbeeld omdat de beheerder van bepaalde koppelnetswerken dezelfde is als de beheerder van een koppelnetswerk dat wel binnen Diginetwerk valt.

De grens van Diginetwerk wordt getrokken rond de netswerken die volledig onder de gedefinieerde afspraken van Diginetwerk vallen.

Paragraaf 3.9 beschrijft de grenzen in plateau 1.

3.3 **Harmonisatie**

3.3.1 *IP-nummerplan en routing*

3.3.1.1 Inleiding

De belangrijkste sturende eisen zijn hier de eenvoud van aansluiting en het minimaliseren van beheer.

We willen bereiken dat (client)systemen van partij X gebruik kunnen maken van services van partij Y. Daarvoor is IP-connectivity nodig tussen het systeem (Host) van partij X en het systeem (Host) van partij Y.

Een belangrijk doel van Diginetwerk is dat d.m.v. éénmalig inrichten van IP-nummerplannen en routeringsafspraken, zoals het instellen van routers etc., een situatie wordt bereikt waarbij niet voor iedere te leggen verbinding alsnog ergens in de keten van tussenliggende netwerken binnen Diginetwerk aanpassingen uitgevoerd hoeven te worden.

3.3.1.2 Eisen/randvoorwaarden

1. Uniceit: Bij iedere op Diginetwerk zichtbare Host hoort één IP-adres, dat uniek is op heel Diginetwerk. Dat unieke IP-adres mag niet geNAT worden binnen Diginetwerk. NAT is wel toegestaan "buiten de randen van Diginetwerk", dus achter de voordeuren van de aangesloten bedrijfsnetwerken.
2. Beveiliging: de te kiezen adressen mogen niet bereikbaar zijn vanaf internet.
3. Beheer: Geen aanpassingen zijn nodig per te leggen verbinding. Er moeten bijv. voldoende IP-adressen beschikbaar zijn, die zodanig te verdelen zijn dat routing in alle koppelnetwerken "eenmalig" is in te regelen.
4. Duidelijkheid: Voor beheerder van (bedrijfs)netwerken mag geen verwarring ontstaan waar een bepaald IP adres zich bevindt, binnen het eigen netwerk, op Diginetwerk of op internet..
5. Standaardisatie; Diginetwerk is bedoeld als een gestandaardiseerde netwerkoplossing voor uitwisselingen op het privacy/beveiligingsniveau Risicoklasse 2 (CBP) dan wel Departementaal Vertrouwelijk (VIR-BI). Voor eventuele hogere eisen kunnen aanvullende maatregelen getroffen worden.

3.3.1.3 Keuzes

IP-nummerplan

Voor heel Diginetwerk bestaat één IP-nummerplan, gebaseerd op z.g. Publieke IP-adressen. Alle adressen aan de randen van Diginetwerk behoren tot dit nummerplan.

Het dekkinggebied van dit nummerplan bepaalt tevens (mede) de grenzen van Diginetwerk. Netwerken die voldoen aan het nummerplan vallen binnen Diginetwerk, de overige netwerken vallen er buiten. Van de Haagse Ring VPN's vallen daarom diverse VPN's buiten de scope van Diginetwerk.

Het nummerplan van Diginetwerk is gebaseerd op een vaste set reeksen IP-adressen. Het eventueel aanpassen van die set is een majeure – en dus ongewenste – wijziging. Organisaties krijgen de IP reeksen door bij het aansluiten op Diginetwerk.

Het beheer van de adresblokken gebeurt getrapt, d.w.z. beheerders van koppelnetwerken beheren het blok van hun koppelnetwerk, en delen subblokken toe aan Organisaties. De onderverdeling van de reeksen naar koppelnetwerken en verder valt buiten de scope van dit document. Organisaties mogen van die adressen gebruik maken voor hun verkeer over Diginetwerk.

Wanneer organisaties veranderen van koppelnetwerk, veranderen ook hun adresreeksen.

Voor Organisaties is Diginetwerk een transparant any-to-any netwerk (feitelijk geldt dat per compartiment, zie verder). Dat betekent dat Organisaties aangesloten aan Diginetwerk elkaar kunnen bereiken via één nummerplan, dus zonder NAT. NAT kan plaatsvinden achter de voordeuren van de bedrijfsnetwerken.

Iedere Organisatie beschikt over een range (subnet) Diginetwerk-adressen. De initiële omvang van die range is afhankelijk van de geschatte behoefte van die Organisatie op een termijn van een paar jaar, onderverdeeld in drie categorieën, groot, middel, klein (ordegrootte 64, 32 en 16 adressen). De range hoort bij de overkoepelende range van het koppelnetwerk. Koppelnetwerkbeheerders beheren de ranges van hun Aangesloten Organisaties.

Alle koppelnetwerken en bedrijfsnetwerken werken momenteel met IPv4. Diginetwerk continueert daarom vooralsnog de thans bestaande praktijk in de diverse koppelnetwerken van IPv4 en is vooralsnog niet gebaseerd op IPv6.

Routing

Diginetwerk hanteert als algemeen principe dat er dynamisch gerouteerd wordt. In plateau 1 wordt daar genuanceerd mee omgegaan.

Routing in de koppelnetwerken gebeurt op basis van de subnetten van de Organisaties. Daarmee zijn de grenzen van de koppelnetwerken en de routingsinformatie simpel en statisch (NB dat grenzen statisch zijn zegt niets over de wijze van routeren). Daarom kan de verantwoordelijkheid voor inrichting van die routing volledig belegd worden bij de beheerder van het betreffende koppelnetwerk.

De verantwoordelijkheid voor en de wijze van inrichten van de routing binnen Koppelnetwerken ligt bij de beheerder van dat koppelnetwerk.

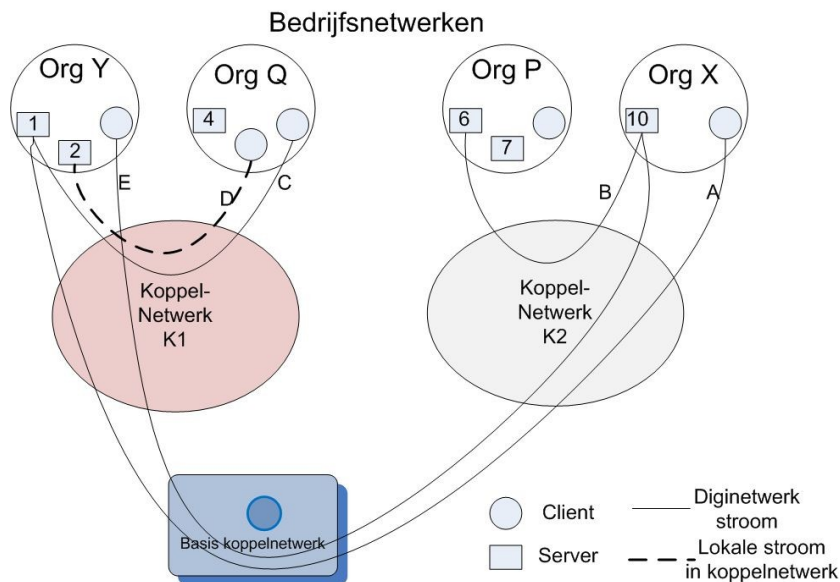
Routing op het BKN gebeurt op basis van de subnetten van de aangesloten koppelnetwerken. Deze routing is statisch. Er is niet gekozen voor dynamische routing, omdat de problematiek van deze statische routing op centraal Diginetwerkniveau (dus BKN) relatief simpel en beheerarm is vanwege het kleine aantal (in eerste instantie 3) koppelingen, en omdat het inrichten van dynamische routing extra eisen stelt aan (de beheerders van) de koppelnetwerken.

In een latere versie van Diginetwerk met meer koppelingen of andere hoeveelheid statische informatie, is dynamische routing wel gewenst. Beheerders van koppelnetwerken kunnen zelf besluiten om in hun netwerk wel dynamisch te routeren.

Keuze plateau 1

Tussen de koppelnetwerken onderling (dus in BKN) wordt statisch gerouteerd op basis van de vastgelegde IP-adresreeksen per koppelnetwerk van het IP-nummerplan.

Alle adressering vanuit (applicatie)systemen vindt plaats op basis van logisch adressen (domeinnamen, URI's), die via DNS vertaald worden naar IP-adressen. Daarmee wordt de vereiste flexibiliteit bereikt om altijd noodzakelijke (sporadische) omnummeringen goed te kunnen ondersteunen. DNS wordt behandeld in paragraaf 3.3.2.



Figuur 5 Routing door koppelnets en BKN

Diginetwerk is – versimpeld weergegeven in figuur 3- opgebouwd uit Koppelnets (K1 en K2) onderling gekoppeld via het BasisKoppelnets (BKN). Aan het Diginetwerk zijn diverse organisaties met hun Bedrijfsnetwerken ("Org") aangesloten via de Koppelnets.

In een bedrijfsnetwerk bevinden zich:

- servers/hosts die alleen zichtbaar zijn in het eigen bedrijfsnetwerk, verder niet interessant voor Diginetwerk;
- Hosts die uitsluitend zichtbaar zijn vanuit (aangesloten op) het eigen Koppelnets (K1), dus uniek (globally unambiguous) adresseerbaar binnen K1. Deze services hoeven niet te voldoen aan Diginetwerk-eisen, en mogen binnen het koppelnets worden voorzien van eventuele eigen adresreeksen.
- Hosts die zichtbaar moeten zijn vanuit heel Diginetwerk, dus uniek adresseerbaar over heel Diginetwerk.

Het is uiteraard de laatste categorie waar Diginetwerk zich primair op richt.

In bovenstaande figuur kan bijvoorbeeld worden gelezen:

K1 = GemnetWAN (een volledig beheerd laag3 netwerk)

K2 = Suwinet (een volledig beheerd laag3 netwerk)

In deze figuur is geschetst dat alle naar services die Diginetwerk-breed worden aangeboden op dezelfde wijze door de diverse koppelnets

worden gerouteerd, zonder NAT etc. Eventuele services die alleen binnen een bepaald koppelnetwerk beschikbaar zijn (service 2 in de figuur) hoeven niet te voldoen aan de Diginetwerk harmonisatie afspraken, als het niet voldoen toegevoegde waarde heeft voor betrokkenen. Formeel gezien valt die stroom dan buiten Diginetwerk.

Hoewel het streven van Diginetwerk nadrukkelijk is om organisaties de mogelijkheid te bieden om met hun éne aansluiting alle services en applicaties etc in de eOverheid te kunnen bereiken, zal dat in plateau 1 nog niet volledig het geval zijn. Er zijn diverse toepassingen die gebonden zijn aan een bepaald koppelnetwerk, hetzij doordat een bepaalde inrichting gekozen is, die niet eenvoudig te migreren is naar het geharmoniseerde Diginetwerk, hetzij omdat een toepassing andere eigenschappen heeft, bijv andere protocollen of andere beveiligingsmaatregelen.

Monitoring en Testvoorzieningen

Diginetwerk is zodanig ingericht wordt dat er (binnen grenzen) open connectivity tussen hosts die zich bevinden aan de randen van Diginetwerk; Diginetwerk is dan een black box. Toch is een belangrijke eis dat er – voor het geval dat “het niet werkt”- mogelijkheden zijn om binnen Diginetwerk de connectivity te testen resp. vast te stellen waar en waarom eventuele problemen ontstaan.

Monitoring, diagnose- en testvoorzieningen kunnen op verschillende lagen worden gepositioneerd. Diginetwerk houdt zich bezig met de lagen tot en met laag 3, dus het gaat om voorzieningen op die lagen, en niet om bijv testvoorzieningen op het niveau van een webservice waarmee vastgesteld kan worden of die service wel werkt.

Er is een aantal gewenste voorzieningen te onderkennen:

1. Diagnose/test voorziening waarmee de correcte werking van een bepaald netwerkgedeelte kan worden vastgesteld. Hierbij kan gedacht worden aan het controleren vanaf bijv. het aansluitpunt van een organisatie aan Diginetwerk of bijv. het BKN bereikt kan worden, en omgekeerd.
2. Een voorziening die de mogelijkheid biedt om langskomend (selectief) verkeer te bekijken, o.a. om daarmee vast te kunnen stellen of een probleem zich voor of na dat punt voordoet.
3. Een voorziening die de mogelijkheid biedt aan alle netwerkbeheerders om te zien of kerndelen van Diginetwerk storingsvrij operationeel zijn, bijv: is koppelnetwerk X beschikbaar.
4. Een voorziening die inzicht biedt in het capaciteitsgebruik van componenten, zowel trendmatig (maandelijkse rapportages) als ad-hoc (is ineens nu alle capaciteit gebruikt).

De term voorziening is in dit architectuurdocument met opzet vaag gehouden, omdat de wijze van implementatie in andere documenten zal worden vastgelegd.

Keuzes

Conform PvU KPS wordt daarom de eis gesteld dat ICMP ECHO pakketten worden doorgelaten. In detail betreft dit Echo (type 8), Echo Reply (type 0) en Time Exceeded (type 11)

ICMP ECHO wordt doorgelaten binnen Diginetwerk.

Er zijn diverse punten binnen Diginetwerk die "pingable" zijn vanuit andere punten in Diginetwerk.

Om ook vanuit het aangesloten bedrijfsnetwerk een punt binnen Diginetwerk te kunnen pingen, en dus diagnoses te kunnen stellen over de grens van bedrijfsnetwerk-diginetwerk heen, wordt aanbevolen om ook daar ICMP ECHO open te zetten, tenminste voor "uitgaande" stromen.

3.3.2

DNS

Adressering van services binnen de eOverheid, dus ook over Diginetwerk is gebaseerd op logische adressering (URI). Er dient daarom een vertaalslag plaats te vinden naar IP-adres. Dat gebeurt d.m.v. DNS. Een korte toelichting op DNS is opgenomen in bijlage 2.

Het gaat concreet om het IP-adres dat gekoppeld is aan de FQDN (Fully Qualified Domain Name), onderdeel van de URI van de service van partij Y.

Hierbij moet het geen verschil maken aan welk koppelnet partij X en Y zijn aangesloten. Als Partij Y (Service Provider) de service heeft gepubliceerd in het Service Register en de FQDN van de service met het unieke IP-adres heeft opgenomen in een DNS, zal iedere Service Consumer daarvan gebruik moeten kunnen maken.

3.3.2.1

Keuzes

DNS op internet of besloten binnen Diginetwerk

Op internet is een uitgebreid DNS stelsel operationeel. Alle overheids-organisaties gebruiken dat stelsel voor hun internetverkeer en vaak ook voor hun overheidsverkeer.

Aangezien Diginetwerk uit beveiligingsoverwegingen volledig gescheiden is van internet, zou de consequentie getrokken kunnen worden om alle DNS informatie in authoritative DNS'en voor services op Diginetwerk ook alleen in een besloten omgeving (en dus niet op open internet DNS'en) uit te voeren. Dat levert echter een ongewenste beheerlast op.

Diginetwerk gaat uit van een én/én oplossing, d.w.z. er kan gewerkt worden met zowel internet DNS als met besloten DNS'en, voor zowel resolving (recursive name server) als authoritative DNS. De Dienstaanbieder (met de overige partners in de keten) bepaalt het risico van de implementatie van de gegevensuitwisseling, en de bijbehorende beveiligingsmaatregelen, waaronder de keuze voor opnemen in besloten eigen authoritative DNS of in internet DNS.

Technisch worden beide DNS-systematieken ondersteund. Omdat een besloten DNS-stelsel een grotere beheerlast met zich meebrengt, en

daarom slechts een zeer beperkt aantal domeinnamen omvat, is internet-DNS de normale basisvoorziening.

Het besloten DNS-stelsel binnen Diginetwerk moet functioneel de volgende mogelijkheden bieden:

Aanbieden

- Een organisatie moet onafhankelijk van het koppelnetwerk (Gemnet, OSB-VPN4, etc.) waarop deze partij is aangesloten, zelf een DNS record op internet kunnen publiceren.
- Wanneer dergelijke organisaties de DNS dienst afnemen van Gemnet of Rijksweb (Rijks-DNS), moeten zij via deze dienst de mogelijkheid hebben om een DNS record op internet te publiceren.
- Een organisatie moet onafhankelijk van het koppelnetwerk (Gemnet, OSB.VPN, etc.) waarop deze partij is aangesloten, wanneer dat vanuit die organisatie of de keten gewenst/vereist is, een DNS record kunnen publiceren via de besloten DNS omgeving waarop deze organisatie is aangesloten (Gemnet DNS of Rijks-DNS).

Afnemen

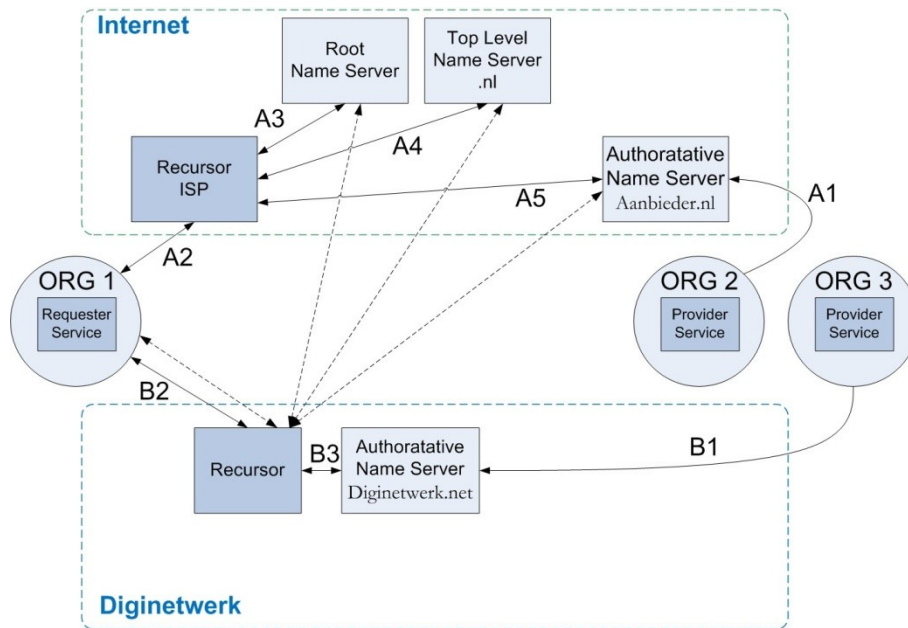
- Een organisatie moet onafhankelijk van het koppelnetwerk (Gemnet, OSB.VPN, etc.) waarop deze partij is aangesloten, DNS records die op internet zijn gepubliceerd kunnen resolvable. Dat gebeurt via de DNS dienst waarvan die organisatie gebruik maakt (Internet DNS, Gemnet DNS of Rijks-DNS).
- Een organisatie moet onafhankelijk van het koppelnetwerk (Gemnet, OSB.VPN, etc.) waarop deze partij is aangesloten, DNS records die binnen de besloten DNS van Gemnet of Rijks-DNS zijn gepubliceerd kunnen resolvable. Dat gebeurt ten minste binnen de 2 DNS domeinen waarvoor de Gemnet DNS en Rijks-DNS naar elkaar verwijzen.

Koppelen

- Voor ten minste een aantal domeinen zullen de Gemnet DNS en Rijks-DNS naar elkaar moeten verwijzen, zodat DNS verzoeken onderling recursief worden afgehandeld.

Deze eisen worden gerealiseerd conform onderstaande schets (Figuur 6).

4 De naam van dit VPN op Haagse ring is nog gebaseerd op de oude naam OSB.



Figuur 6 De DNS oplossingen in Diginetwerk

In deze figuur is een aantal publicatie/resolving modellen opgenomen, die ondersteund worden binnen Diginetwerk:

- **Publicatie in een internet authoritative DNS**
Organisatie ORG2 publiceert zijn service, bijv service1.aanbieder.nl, in de DNS op internet die authoritative is voor zijn domein "aanbieder.nl", aangegeven met A1. Als organisatie ORG1 die service wil gebruiken zijn er twee mogelijkheden. ORG1 resolveert direct via de internet recursive DNS bijvoorbeeld van zijn ISP, aangegeven met A2. Die recursor doet vervolgens de resolving via het normale internet DNS-stelsel (A3-A5). Alternatief voor ORG 1 is om de besloten recursor van Diginetwerk te bevragen voor de service van ORG2. Aangezien die besloten recursor niet kan resolvable in het besloten domein "diginetwerk.net" zal de resolving vervolgens uitgevoerd worden op internet (gestippelde lijnen; of eventueel via een forward naar een ISP DNS).
- **Publicatie in de besloten authoritative DNS van Diginetwerk**
Organisatie ORG 3 publiceert zijn service, bijv service2.org3.diginetwerk.net in de besloten DNS (B1). Als ORG 1 die service wil gebruiken kan geen resolving via internet plaats vinden. ORG1 moet dus naar de besloten recursor toe (B2). Dat kan omdat ORG1 een conditional forward heeft voor het domein (zone) Diginetwerk.net, en dus alleen voor dat domein naar de besloten recursor gaat, of omdat ORG 1 voor alle resolving naar de besloten recursor gaat. De besloten recursor gaat vervolgens direct naar de besloten authoritative DNS (B3).

In het totaal van Diginetwerk bestaan in plateau 1 twee besloten DNS'en, die onderling gekoppeld zijn. RIJKSDNS is authoritative voor diginetwerk.net en de Gemnet DNS is authoritative voor int-gemnet.nl. beide recursor bevatten conditional forwards naar zowel het domein int-gemnet.nl als diginetwerk.net. De werking blijft gelijk.

3.4 Beveiliging

3.4.1

Inleiding

Beveiliging betreft Beschikbaarheid, Exclusiviteit en Integriteit.

De eisen aan de beveiligingsniveaus vloeien voort uit de rubricering van de gegevens (risicoklassen van de WBP), en die is weer van invloed op de classificatie van de voorziening, gezien vanuit de afhankelijkheid van een organisatie van de betreffende voorziening.

Goede beveiliging is een van de bestaansvoorwaarden van Diginetwerk. Er wordt nog gewerkt aan nader uitgewerkte InformatieBeveiligingskaders voor de hele keten van Diginetwerk, inclusief tactische Normenkaders. Diginetwerk zal zich gezien de aard van het besloten netwerk richten op de hogere classificaties, niveaus 2 en 3 op een schaal van 0-3, z.:

- Beschikbaarheid: **Wezenlijk** (Nauwelijks uitval gedurende de openingstijden) en **Onmisbaar** (Slechts in uitzonderlijke gevallen niet operationeel);
- Exclusiviteit: **Cruciaal** (Gegevens alleen toegankelijk voor direct betrokkenen) resp. **Dwingend** (Bedrijfsbelangen worden ernstig geschaad als ongeautoriseerden toegang krijgen);
- Integriteit: **Detecteerbaar** (Een zeer beperkt aantal fouten is toegestaan) resp. **Onontbeerlijk** (Bedrijfsproces eist foutloze informatie).

Zie bijlage III.

In paragraaf 1.3 is het relevante NORA-2 principe weergegeven: Het principe stelt dat bij voorkeur alle communicatie tussen overheidsorganisaties verloopt via besloten netwerken.

Dit wordt als volgt concreet gemaakt voor Diginetwerk:

Wanneer communicatie tussen overheidsorganisaties vanwege de specifieke beveiligingseisen een besloten netwerk vereist, dan zal gebruik gemaakt worden van Diginetwerk.

Wanneer die specifieke eisen niet gelden voor een bepaalde verkeersstroom is de keuze voor Diginetwerk of internet vrij te maken door betrokken organisaties, bijv op basis van standaardisatie.

"Diginetwerk MOET waar vereist vanuit beveiliging, Diginetwerk MAG waar gewenst vanuit standaardisatie."

NORA principe AP32, AP 33 en AP 34 vereist dat de dienst voldoet aan een kwaliteitsbaseline, en als afgeleide is gesteld t.a.v. Betrouwbaarheid: "De beschikbaarheid en de kwaliteit van diensten voldoet aan vooral bepaalde normen." NORA principe AP29 en AP 33 vereist dat de wijze waarop een dienst wordt geleverd kan worden verantwoord.

Diginetwerk is opgebouwd uit koppelnetswerken, die ieder op zich voldoen aan de eisen van WBP 2/3 en aan de eisen van de eOverheid m.b.t. afhankelijkheid.

De nog uit te werken IB-kaders, Normenkaders en verantwoordingskaders hebben vooral te maken met harmonisatie tussen koppelnetswerken en controleerbaarheid meer dan met het daadwerkelijk op niveau brengen van het beveiligingsniveau.

Diginetwerk legt nadruk op een aantal beveiligingsmaatregelen, gericht op het verhogen van Beschikbaarheid, Exclusiviteit en Integriteit:

1. Binnen Diginetwerk zijn geen Single Points of Failure.
NB De koppeling tussen een organisatie en Diginetwerk valt hier buiten. Die koppelingen mogen enkelvoudig zijn, wanneer de betreffende organisatie daarvoor kiest.
2. Diginetwerk is volledig gescheiden van internet.
Diginetwerk is nergens gekoppeld aan internet. De IP-adressen die toegelaten worden op Diginetwerk worden niet gerouteerd op internet.
3. Binnen Diginetwerk bestaat in principe de mogelijkheid om gedeelten van Diginetwerk af te scheiden van andere gedeelten. Dit wordt compartimentering genoemd.

3.4.2 *Compartimentering en Zones*

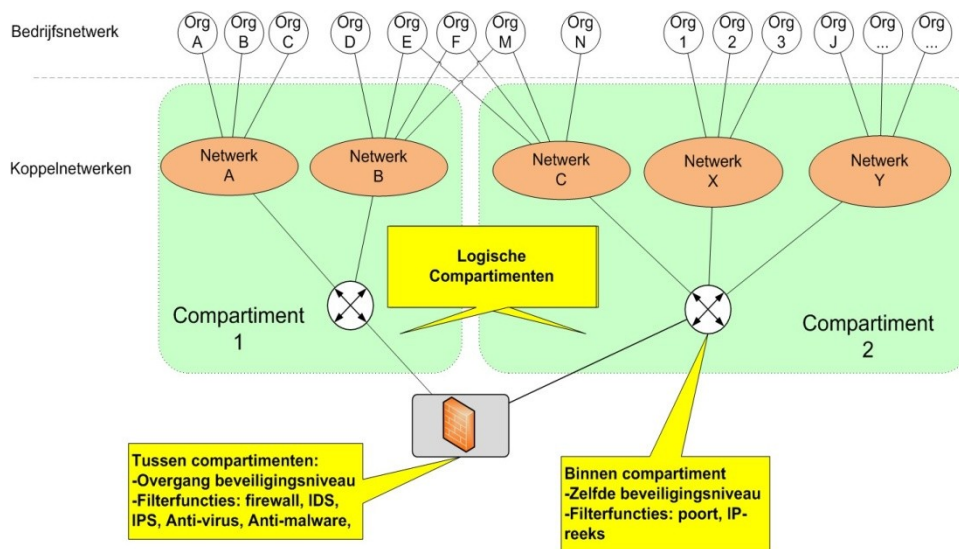
Diginetwerk bestaat uit een aantal onderling gekoppelde koppelnetswerken. Het doel van Diginetwerk is het bieden van een betrouwbare, veilige, beheerarme koppeling tussen alle overheidspartijen. Een optimale keuze is noodzakelijk tussen enerzijds volledig vrij verkeer tussen alle aangesloten organisaties (voordeel: net als bij internet geen belemmeringen in het pad tussen die twee) en anderzijds de huidige situatie waarbij op allerlei punten, bijvoorbeeld op grenzen tussen beheerdomeinen etc complexe belemmeringen bestaan. Gekozen is daarom – conform Nora Informatie Beveiliging – voor het concept van compartimenten of zones. Binnen een zones is vrij verkeer mogelijk, en tussen zones, op het grensvlak, zijn beveiligingsmaatregelen van kracht.

Nora Informatie beveiliging

Conform “NORA Normen Informatiebeveiliging ICT-voorzieningen” (zie citaat in bijlage I) en NORA principe AP37 wordt uitgegaan van zonering in verschillende zones.

3.4.3 *Toepassing in Diginetwerk*

Diginetwerk onderkent zones als gedefinieerd in NORA IB-normen. Een zone komt overeen met een (koppel)netwerk. Op zonegrenzen worden bepaalde vormen van filtering toegepast. Diginetwerk voegt aan het principe van zonering nog het concept van Compartimenten toe. Een compartiment is een netwerkgedeelte met hetzelfde beveiligingsniveau, dat kan bestaan uit delen die beheerd worden door verschillende beheerders (dus verschillende koppelnetswerken), en daardoor dus bestaat uit verschillende zones. De filterfuncties op zonegrenzen binnen een compartiment verschillen van de functies op compartimentsgrenzen, zie paragraaf 3.4.3.1 .



Figuur 7 Compartimenten in Diginetwerk

Compartimenten binnen het Diginetwerk zorgen voor de logische scheiding. Dat betekent dat alleen partijen die binnen het zelfde compartiment koppelen, rechtstreeks met elkaar kunnen communiceren. Met rechtstreeks wordt hier bedoeld dat er geen aanpassingen in filterfuncties of routing binnen Diginetwerk nodig zijn. Communicatie tussen endpoints in verschillende compartimenten is uitsluitend selectief mogelijk via strengere filterfuncties (Source-destination paren) die beveiligings- en/of schoningsvoorzieningen bevatten.

Compartimenten in Diginetwerk moeten bestaan uit meer dan één zone (koppelnetwerk).

Wanneer een compartiment bestaat uit één koppelnetwerk met een afwijkend beveiligingsniveau is het de vraag of dat afwijkende koppelnetwerk wel beschouwd kan worden als onderdeel van Diginetwerk. Om de grenzen van Diginetwerk eenduidig te kunnen trekken wordt een dergelijk afwijkend koppelnetwerk niet beschouwd als behorend tot Diginetwerk. Pas als een compartiment bestaat uit (delen van) meerdere koppelnetswerken, die wel passen binnen het nummerplan, wordt dat compartiment beschouwd als onderdeel van Diginetwerk. In plateau 1 doet zich dat niet voor.

Duidelijk zal zijn dat compartimenten veel voordelen bieden. Er moeten echter niet te veel compartimenten onderkend worden. De connectiviteit daalt dan, het beheer neemt sterk toe evenals de complexiteit. Het aantal compartimenten dient daarom zo laag mogelijk gehouden te worden. De hierbij gehanteerde richtlijn is dat een (extra) compartiment alleen bestaansrecht heeft wanneer dit vanuit een beveiligingsoptiek kan worden aangetoond.

3.4.3.1

Beveiliging tussen Compartimenten

Conceptueel is er sprake van compartimenten, ieder bestaande uit zones met eenzelfde beveiligingsniveau.

Aangesloten organisaties die onderling willen koppelen kunnen zich

1. ofwel beide in dezelfde zone bevinden Org A en Org B in Figuur 7),
2. ofwel in verschillende zones binnen hetzelfde compartiment (Org A en Org D)
3. ofwel in twee verschillende compartimenten (Org A en Org 1).

Theoretisch kan een koppelnetwerk een zone hebben in compartiment X en ook een zone in compartiment Y. Dit maakt voor het concept niet uit.

Op Diginetwerk worden de netwerken Gemnet, Suwinet, Haagse Ring-OSB-VPN beschouwd als behorend tot één compartiment. Het beveiligingsniveau van die netwerken is gelijkwaardig. Er kan binnen dat compartiment onderling worden gecommuniceerd zonder extra filterfuncties. Dat compartiment wordt aangeduid met "compartiment WBP-2". De koppelnetwerken zijn echter verschillende zones, vanwege de andere beheerverantwoordelijkheid.

Binnen de Haagse Ring is sprake van verschillende compartimenten binnen (het ene beheerdomein van) de Haagse Ring.⁵ Zoals eerder aangegeven worden deze compartimenten en zones niet beschouwd als behorend tot Diginetwerk.

In principe (dus nog niet in plateau 1) is communicatie tussen compartimenten met verschillend beveiligingsniveau is mogelijk. Hiervoor is grensbewaking op de koppelvlakken tussen de compartimenten nodig.

3.4.4

Eisen/randvoorwaarden aan beveiliging tussen compartimenten/zones

1. Diginetwerk bestaat uit een aantal beveiligingscompartimenten en zones.
2. Partijen/onderdelen binnen een compartiment hebben een gelijkwaardig beveiligingsbeleid resp. beveiligingsniveau.
3. Partijen/onderdelen binnen een compartiment vormen een onderling trustdomein.
4. Binnen een compartiment bestaat een hoge mate van uitwisselingsvrijheid "alles staat open" wat toegestaan is binnen Diginetwerk.
5. Tussen compartimenten zijn maatregelen getroffen die de risico's van verschillen tussen de compartimenten adequaat opvangen.
6. Compartimenten hoeven niet "samen te vallen" met een gehele partij; het beveiligings-/trustniveau voor bijv. OSB-verkeer naar een partij zal anders kunnen zijn dan voor samenwerkingsapplicaties van diezelfde partij.

⁵ *Definitie van Compartimenten uit GOUD:* Compartimentering is het gebeuren dat delen van de ICT infrastructuur afgeschermd zijn of worden van andere delen van de ICT infrastructuur. Een compartiment beschermt de resources daarbinnen op netwerkniveau en ontsluit deze resources op een gecontroleerde manier. Concreet bestaat een compartiment uit één of meer VLAN's of LAN's welke worden beveiligd en afgeschermd van de overige infrastructuur middels een beveiligd koppelvlak

3.4.4.1 Keuzes

Er wordt onderscheid gemaakt naar soort samenwerking, te weten

-Tussen organisaties, loosely coupled (zie paragraaf 2.6), waarbij weinig interactie mogelijk is, hierop is het beveiligingskader van Diginetwerk van toepassing.

-Tussen ambtenaren, tightly coupled, waarbij intensieve samenwerking, toegang tot file servers, diverse protocollen etc. mogelijk is. Hierop is het beveiligingskader van DWR van toepassing. Dit wordt hier niet verder behandeld, anders dan dat als gevolg van DWR beveiligingskaders op bepaalde VPN's van Haagse Ring (bijv. Rijksweb VPN) een ander beveiligingsniveau en -regime van toepassing is. Die VPN's maken nu geen deel uit van Diginetwerk.

Filterfuncties

We onderscheiden een aantal niveaus van maatregelen die genomen kunnen worden op het koppelvlak tussen de koppelnetwerken resp. koppeling naar organisaties:

1. Pakketfiltering: filteren op poort en IP adresreeksen
2. Pakketinspectie: firewall (d.w.z. source-destination pairs) en IDS
3. Applicatie inspectie: Proxy server, Firewall en IDS
4. Applicatie inspectie content screening: content screening, Proxy server, Firewall en IDS

Binnen Diginetwerk worden vooralsnog alleen de beveiligingsniveaus gericht op gegevensclassificatie "Basis" (WBP Risicoklasse 2) en "Hoog" (Dep Vertrouwelijk) onderkend.

Bij uitwisseling van informatie binnen hetzelfde compartiment, of naar een "lager" compartiment, worden maatregelen ad 1 toegepast op de koppelvlakken tussen zones (koppelnetwerken).

Bij uitwisseling van een lager naar een hoger compartiment worden maatregelen ad 2 toegepast.

Bij uitwisseling met partijen buiten Diginetwerk worden maatregelen ad 3 en 4 toegepast.

Indien er verkeer van een lager compartiment gestuurd wordt naar een hoger gelegen compartiment dient er pakketinspectie uitgevoerd te worden.

Indien verkeer van een hoger gelegen compartiment gestuurd wordt naar een lager gelegen compartiment volstaat pakketfiltering.

In Plateau 1 wordt dit als volgt geïmplementeerd:

De koppelnetwerken Gemnet, Suwinet, OT-wolk en RINISnet alsmede het OSB-VPN op Haagse Ring maken deel uit van één compartiment met basis-beveiligingsniveau van Diginetwerk, gericht op WBP-risicoklasse 2. Deze netwerken kunnen daarom any-to-any met elkaar uitwisselen. Er vindt altijd Pakketfiltering plaats op de grenzen van netwerken (zones). De filtering houdt hier in dat er wordt gefilterd op protocol resp poort (alleen HTTP(s), FTP, SMTP, DNS toegestaan) en op IP-range (alleen de Diginetwerk-ranges toegestaan).

Naar keuze van de beheerder van het koppelnetwerk kan op de rand van een koppelnetwerk een Intrusion Detection System (IDS) ondergebracht worden, mits dat geen belemmeringen oplevert voor nieuwe verbindingen resp. stromen.

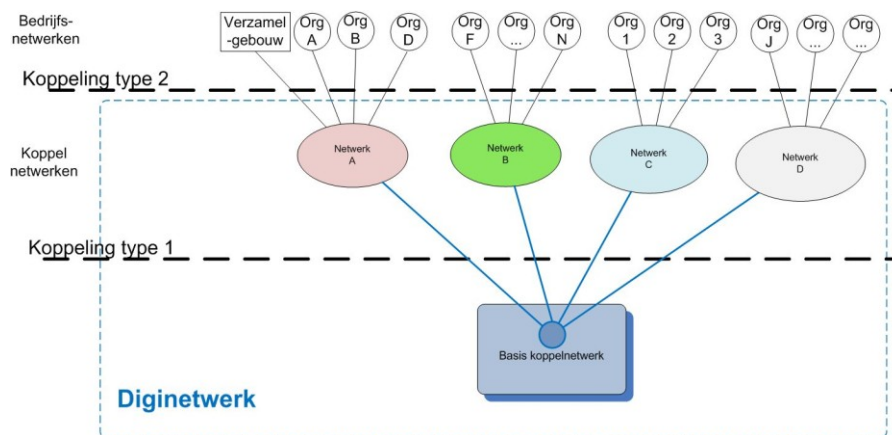
Bij de overgang naar een ander beveiligingsniveau (bijv. DEP-V VPN op Haagse Ring) vindt ook pakketinspectie plaats in een firewall, d.w.z. alleen de expliciet toegestane combinatie van source en destination wordt doorgelaten.

In plateau 1 is er alleen op de Haagse Ring sprake van verschillende beveiligingsniveaus. Alleen bij de overgang van/naar VPN's met hoge beveiliging op de Haagse ring (m.u.v. OSB-VPN) is daarom deze pakketinspectie ingericht. Dat gebeurt in RijksConnect.

3.5 Onderlinge koppeling van netwerken

3.5.1 Inleiding

Het concept van Diginetwerk gaat uit van onderling geharmoniseerde en onderling gekoppelde koppelnetwerken, die organisaties any-to-any connectivity mogelijk maken tussen aangesloten organisaties resp. bedrijfsnetwerken. Harmonisatie is in de vorige paragrafen beschreven. Deze paragraaf beschrijft de architectuur van de onderlinge koppelingen.



Figuur 8 Koppelingen in Diginetwerk

Diginetwerk onderkent drie soorten netwerken: Bedrijfsnetwerken, koppelnetwerken en het BasisKoppelNetwerk. Tussen die drie soorten netwerken zijn twee hoofdtypen koppeling te onderkennen, zie ook bovenstaande figuur:

- Type 1, de koppeling tussen koppelnetwerken en het BKN; dit type wordt in paragraaf 3.6 uitgewerkt.
- Type 2, de koppeling tussen bedrijfsnetwerken en de koppelnetwerken; dit type wordt behandeld in paragraaf 3.7.

Er is dus geen koppeling tussen een bedrijfsnetwerk en het BKN. De reden hiervoor is dat daarmee BKN zeer beperkt, onderhoudsarm en robuust gehouden kan worden.

De belangrijkste functionaliteit van dit stelsel van koppelingen (koppelnetswerken en BKN) is het mogelijk maken van any-to-any IP-verkeer binnen Diginetwerk.

3.5.2

Uitgangspunten koppelingen

Bedrijfsnetwerken zijn de netwerken van een organisatie. Dergelijke bedrijfsnetwerken kunnen zeer complex zijn, denk aan netwerken van grote gemeenten, Justitie of V&W. Door een organisatie aangeboden services/servers bevinden zich in principe binnen die eigen bedrijfsnetwerken. Hierop komen diverse varianten voor bijv ASP of samenwerkingsverbanden.

Koppelnetswerken zijn netwerken waarop bedrijfsnetwerken zijn aangesloten. Die koppelnetswerken zijn bedoeld om connectivity tussen bepaalde groepen organisaties mogelijk te maken. Streefsituatie van Diginetwerk is dat iedere Organisatie slechts op één koppelnetswerk per compartiment is aangesloten. Daarmee wordt bedoeld dat als een organisatie deel uitmaakt van twee compartimenten (dus met een verschillend beveiligingsniveau) dan zal die organisatie in het algemeen op beide een aansluiting hebben.

Het **BasisKoppelNetwerk** is het onderlinge koppelpunt voor de koppelnetswerken. Aan het BKN worden geen bedrijfsnetwerken aangesloten, alleen koppelnetswerken.

Laag 3

Alle netwerken in/aan Diginetwerk eindigen op laag 3 (router).

Het eindigen op laag 3 is nodig voor bedrijfsnetwerken omdat alleen op die wijze een eenduidige scheiding van het beheer van het betreffende netwerk gerealiseerd kan worden. De betreffende beheerder is immers verantwoordelijk voor "zijn" laag 3 nummerplan en wat daar bij hoort.

Het eindigen op laag 3 geldt ook voor koppelnetswerken omdat ook daar een beheerverantwoordelijkheid ligt, maar ook omdat een laag 2 koppelnetswerk de beheerlast van routing bij de koppelrouters van de aangesloten netwerken zou leggen.

Tussen twee van die koppelrouters die beheerde laag 3 netwerken begrenzen bevindt zich een laag 2 verbinding.

3.6

Koppelingen met BKN, type 1

Deze paragraaf beschrijft de architectuur van de koppeling tussen koppelnetswerken onderling op het BKN.

3.6.1

Eisen/randvoorwaarden BKN

- Koppeling van een koppelnetwork met BKN moet hoog beschikbaar zijn en moet daarom redundant, geografisch gescheiden en met automatische failover ingericht worden.
- Demarcatiepunten zijn éénduidig bepaald, beheer is eenduidig belegd.
- Er zijn voorzieningen voor monitoring van het verkeer aanwezig, waardoor o.a. bepaald kan worden of een storing zich aan de ene of aan de andere kant van een demarcatie lijn bevindt, ofwel er kan vastgesteld worden in welk koppelnetwork een storing zich bevindt.

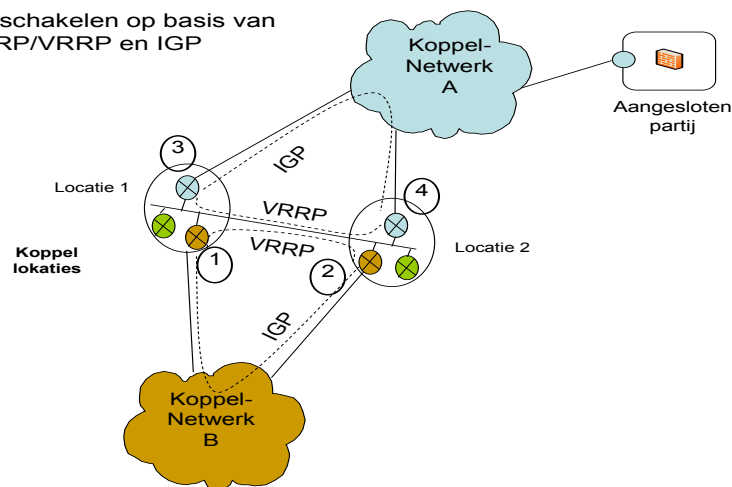
3.6.2

Keuzes

BKN wordt ingericht als een Sterkoppeling (en niet als Maas of Wolk). Er is gekozen om BKN in plateau 1 onder te brengen in 2 aparte locaties die overeen komen met de locaties waar de reeds eerder gerealiseerde koppeling tussen Suwinet en Gemnet al was gerealiseerd.

Failover: Omdat BKN wordt ingericht als een ster, waarbij alle te koppelen netwerken op één (redundant) punt bij elkaar komen, moet de wijze van koppelen en failover daarom voor alle netwerken (op een aantal punten) gelijk zijn. Dat betreft met name de keuze tussen een dynamisch Routing Protocol (eBGP⁶) versus een failoverprotocol (HSRP⁷ of VRRP⁸).

Omschakelen op basis van HSRP/VRRP en IGP



Figuur 9 Omschakelen op basis van HSRP/VRRP en IGP

Gekozen is nu (komende 2 a 3 jaar) voor het gebruik van HSRP/VRRP (Figuur 9) en niet voor external BGP (eBGP) op BKN. Redenen hiervoor zijn:

⁶ eBGP: External Border Gateway Protocol, voor uitwisseling routeringsinformatie tussen verschillende Autonomous Systems (AS)

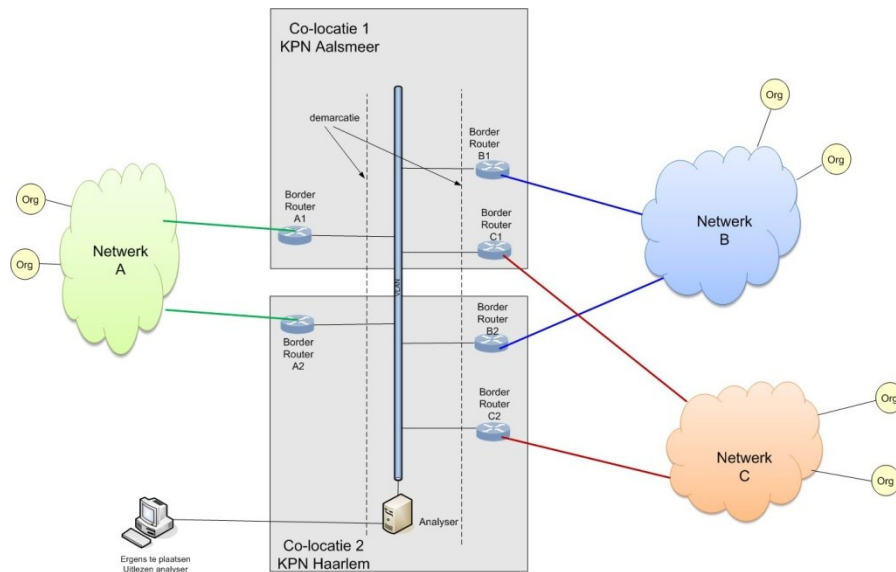
⁷ HSRP: Hot Standby Router Protocol, een Cisco proprietary protocol om een fout-tolerante default gateway op te zetten.

⁸ VRRP: Virtual Router Redundancy Protocol, een non-proprietary protocol voor fout-tolerante gateway.

- Beheer van een aantal koppelnetwerken is thans niet gebaseerd op BGP.
- BGP werkt niet met alle koppelconstructies, met name niet wanneer een firewall als buitenste punt van een netwerk vereist wordt.

Uitgangspunt: Een van de twee locaties is een primaire locatie voor alle koppelnetwerken, die onder normale omstandigheden 100% van het gebruikersverkeer afhandelt, en de andere is een secundaire, die onder normale omstandigheden 0 % afhandelt. De primaire locatie is primair voor alle netwerken en verkeerssoorten. Welke locatie primair en welke secundair is wordt bepaald door configuratie.

Wanneer in een failover situatie omgeschakeld wordt van de ene koppelrouter (bijv. 1) naar de andere (bijv. 2), zal ook automatisch vanuit het netwerk zelf naar de andere koppelrouter omgeschakeld of geherrouteerd moeten worden. Het is niet gewenst dat de actieve kant aan de buitenkant een andere is dan de actieve kant van de binnenkant. Dit automatisch omschakelen van het uitgaande verkeer van een koppelnetwerk, wordt per koppelnetwerk geregeld op basis van een per netwerk door de netwerkbeheerder zelf te kiezen protocol. Onderlinge afstemming resp. communicatie daarover tussen koppelnetwerkbeheerders en BKN-beheerder resp Diginetwerk regisseur is wenselijk om verwachtingen over failover reactietijden te managen. Met failover reactietijden wordt de gehele tijd bedoeld die nodig is om alle componenten om te laten schakelen. Naar verwachting zullen – afhankelijk van de inrichting van het koppelnetwerk – keuzes, timers etc. verschillen resulterend in mogelijk verschillende reactietijden van de diverse netwerken. Gemikt wordt op een redelijke omschakeltijd van enige minuten maximaal. De eisen aan fail-back, d.w.z. wanneer en hoe snel wordt weer teruggeschakeld naar de oorspronkelijke primaire situatie wanneer storingen hersteld zijn, moeten nog vastgesteld worden. Fail-back levert immers ook weer een korte onderbreking op. Terugschakelen in een onderhoudswindow is daarom gewenst.



Figuur 10 Globale inrichting BKN

Samenvattend is de routing in BKN op basis van de ranges van het destination-koppelnetwerk statisch ingericht en de failover (exit- én koppelrouter) automatisch.

Ontwerpeis: De keuze voor HSRP/VRRP oplossing aan de BKN kant van bijv. OTwolk heeft geen invloed op de HSRP/VRRP vs eBGP keuze aan de andere kant van OTwolk, bijv voor de koppeling met een hosting provider.

Keuzes t.a.v. onderlinge koppelingen

De verbindingen tussen een koppelnetwerk en BKN zijn ofwel:

- uitlopers van het betreffende koppelnetwerk, d.w.z. de verbinding wordt beheerd door de beheerder van het koppelnetwerk.

- een aparte verbinding die wordt geleverd door een ander koppelnetwerk.

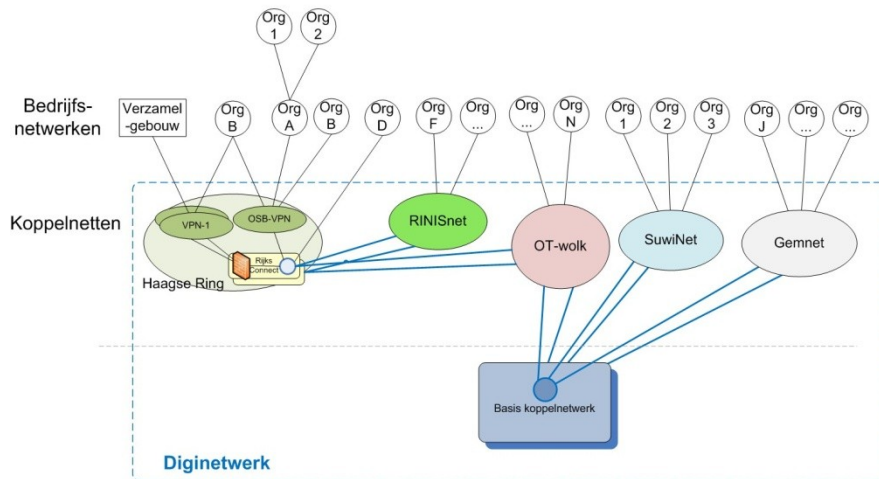
Bijv: de verbinding tussen RijksConnect/Haagse Ring en BKN wordt geleverd door de OTwolk. Op die manier kunnen mogelijk getrapte koppelingen ontstaan. De reden voor een dergelijke keuze is vaak pragmatisch (kosten, contracten).

In (aan) het BKN worden direct onderling gekoppeld de koppelnetwerken Gemnet, Suwinet en OTwolk. Via de OTwolk en RijksConnect zijn de Haagse Ring VPN's gekoppeld.

De Haagse Ring VPN's zijn onderling gekoppeld via RijksConnect.

Haagse Ring/RijksConnect is te beschouwen als een cluster van onderling gekoppelde koppelnetwerken. Organisaties (bedrijfsnetwerken) kunnen ofwel rechtstreeks aansluiten aan een (of meer) VPN's, wanneer ze voldoen aan de aansluitvoorwaarden, ofwel aan RijksConnect wanneer dat niet het geval is. Daardoor zijn er op dat cluster meer variaties in aansluitmogelijkheden dan bij de meeste andere koppelnetwerken.

Koppelingen in Release 1



Figuur 11 Onderlinge koppelingen in plateau 1 type 1

3.7 Koppeling Organisatie aan Diginetwerk, type 2.

3.7.1 Inleiding

Deze paragraaf beschrijft de architectuur van de koppeling tussen het bedrijfsnetwerk van een Aangesloten Partij en het gekozen Koppelnetwerk.

Idealiter heeft een organisatie maar één toegangsroute van/naar Diginetwerk. In de praktijk zijn er diverse redenen waarom daar van afgeweken zal worden. Bijv. omdat organisaties willen aansluiten aan netwerken in verschillende compartimenten (bijv RIJKSweb-VPN vs OSB-VPN), of in de waarschijnlijk langdurige migraties van het ene netwerk naar het andere.

Andere redenen waar we niet altijd invloed op hebben, kunnen zitten in juridische/contractuele voorwaarden.

Daarom hanteert Diginetwerk een meer genuanceerd uitgangspunt.

Een Organisatie kan aan meer dan één koppelnetwerk aansluiten. Een Service van die organisatie wordt echter altijd ontsloten via één IP-adres, dat ofwel behoort bij het ene, ofwel bij het andere netwerk. Routing vanaf een afnemer naar die service gaat dan via de "normale" routeringsregels, d.w.z. het koppelnetwerk waarop de afnemer is aangesloten, routeert statisch naar bijv. BKN en vervolgens naar het juiste koppelnetwerk.

Uitgangspunt is hierbij dat de afnemer zijn eigen uitgaande routing verzorgt. Als een afnemer is aangesloten aan twee koppelnetwerken, is de afnemer verantwoordelijk voor de routing vanuit zijn eigen bedrijfsnetwerk naar het gewenste koppelnetwerk. Die keuze is in principe

vrij, zij het dat de betreffende koppelnetwerkbeheerder richtlijnen of voorschriften kan hebben.

Als een aanbieder een service/server wil ontsluiten op meer dan één koppelnetwerk (bijv in een migratietraject), zal die (virtuele) server twee IP-adressen (NIC's) moeten hebben. Daarbij geldt als randvoorwaarde dat het niet mogelijk mag zijn om de server te gebruiken om via die server van het ene naar het andere netwerk te komen ("non-transit").

In bovenstaande tekst is aangegeven dat het weliswaar mogelijk is om aan meerdere koppelnetwerken aan te sluiten, maar dat een dergelijke meervoudige aansluiting extra complicaties introduceert. Daarom wordt als uitgangspunt aangehouden dat een organisatie in principe aan slechts één koppelnetwerk is aangesloten.

3.7.2

Eisen/randvoorwaarden

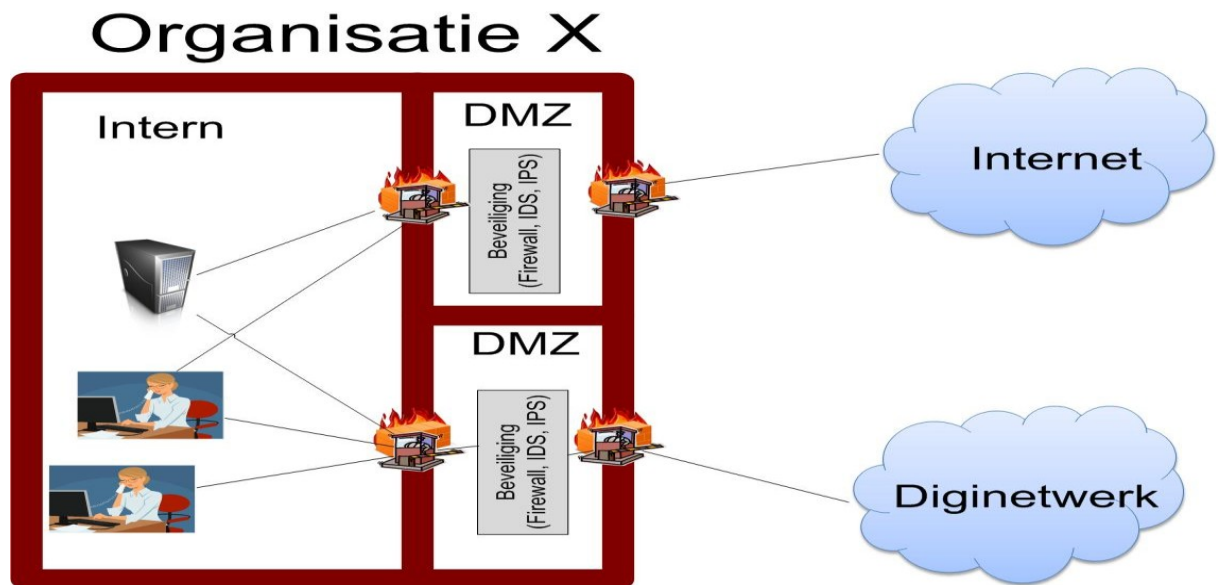
- Een organisatie kiest zelf voor aansluiting op een bepaald koppelnetwerk. De keuze kan bepaald worden door beschikbare diensten, kosten etc..
- Een belangrijk deel van de aansluit- en gebruiksvoorwaarden worden afgesproken tussen organisatie en koppelnetwerkbeheerder. Bijvoorbeeld Koppeling van een partij met een koppelnetwerk kan een zeer hoge beschikbaarheid hebben, d.w.z. redundant en met automatische failover ingericht, maar kan ook met een enkelvoudige hoge beschikbaarheid hebben.
- Er mag geen directe koppeling bij de aangesloten organisatie tussen Diginetwerk en internet bestaan. (Algemene beveiligingseis van Diginetwerk, zie 3.4.1 punt 2.
- Alle services/servers die worden aangeboden vanuit het bedrijfsnetwerk zijn adresseerbaar op het koppelvlak tussen bedrijfsnetwerk en koppelnetwerk op basis van het Diginetwerk IP-nummerplan. Er wordt dus pas eventueel geNAT achter dat koppelvlak.
- De organisatie draagt zelf zorg voor internet toegang tot crl en DNS.

3.7.3

Partij met Diginetwerk, achter de voordeur

Het is sterk aan te bevelen om zg IP-reducerende maatregelen te treffen, door bijv achter de voordeur te werken met een reverse proxy, load balancer e.d.. Daarmee kan het aantal te beheren kanalen van buiten gereduceerd worden en daarmee wordt tevens aan de buitenkant zichtbare IP-adressen geminimaliseerd.

De meeste organisaties zullen zowel een aansluiting op Internet hebben als op Diginetwerk. Diginetwerk verbiedt een koppeling tussen Diginetwerk en Internet.



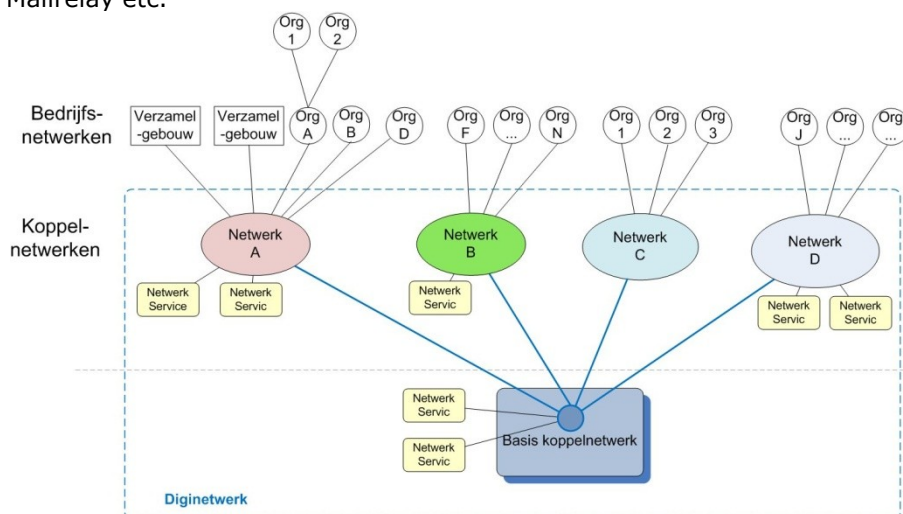
Figuur 12 Gescheiden aansluiting op Internet en Diginetwerk

Ook al vindt het verkeer plaats via Diginetwerk, dan zal internet toegang nodig zijn ivm DNS resolving (tenzij een besloten DNS gebruikt wordt) en voor crt-checking vanuit Organisaties. In plateau 1 is dat een verantwoordelijkheid van de betreffende organisatie zelf.

3.8 NetworkServices

3.8.1 Inleiding

De kern van Diginetwerk is connectiviteit. Om die connectiviteit goed te kunnen gebruiken zijn ook infrastructurele services nodig, zoals DNS, Mailrelay etc.



Figuur 13 Networkservices conceptueel

3.8.2

Eisen/randvoorwaarden

Services kunnen bestaan per koppelnetwerk.

Ze kunnen onderling gekoppeld zijn.

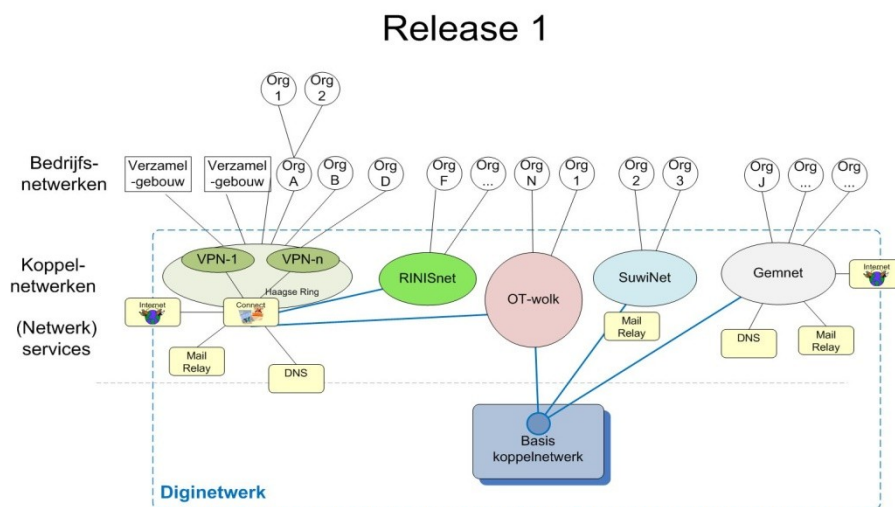
Diginetwerk-brede services zijn in principe ook mogelijk. In Plateau 1 wordt daar nog geen gebruik van gemaakt.

3.8.3

Keuzes

In plateau 1 zijn de services (nog) ondergebracht per koppelnetwerk, en zijn ze waar nodig onderling gekoppeld.

Onderling gekoppeld zijn Rijks DNS met DNS Gemnet (zie paragraaf 3.3.2)

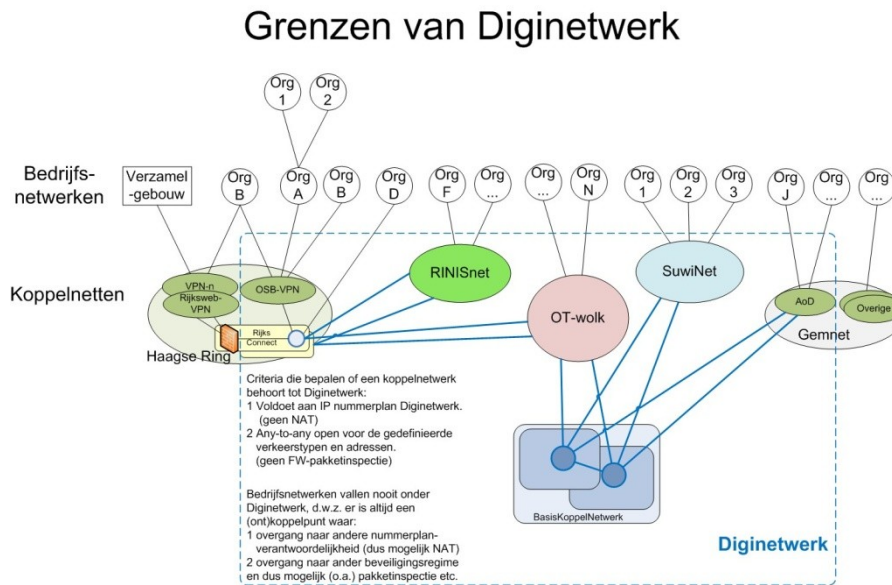


Figuur 14 positionering Services in Plateau 1

NTP-services worden vooralsnog niet centraal in Diginetwerk gepositioneerd maar bestaan in de diverse (koppel)netwerken. Dat kan mits alle NTP-tijden direct afgeleid zijn van de (Europese) atoomklok.

3.9 Grenzen van Diginetwerk in plateau 1

In paragraaf 3.2.1 is aangegeven dat de grenzen van Diginetwerk helder moeten zijn. De grenzen worden bepaald doordat alleen die koppelnetwerken die volledig voldoen aan de afspraken van Diginetwerk behoren tot Diginetwerk. Onder koppelnetwerken worden verstaan de zelfstandige delen (zones, VPN, CUG) van netwerken, zie ook onderstaande figuur.



Figuur 15 Grenzen van Diginetwerk

Dit vertaalt zich in de volgende hoofdcriteria die bepalen of een koppelnetwerk deel uitmaakt van Diginetwerk:

- Behoort het IP-nummerplan van het betreffende netwerk tot het IP-plan van Diginetwerk.
- Zijn er geen barrières voor het Diginetwerkverkeer op de koppeling van het koppelnetwerk met de rest van Diginetwerk.

Indien op beide vragen positief geantwoord wordt, behoort het koppelnetwerk tot Diginetwerk.

De koppelnetwerken binnen Diginetwerk zijn nog bezig met diverse aanpassingen aan de nieuwe structuur en afspraken van Diginetwerk. De hier beschreven grenzen kijken naar de streefsituaties binnen de betreffende koppelnetwerken.

Diginetwerk plateau 1 bestaat uit

- -BKN
- de koppelnetwerken:
 - Haagse Ring OSB-VPN
 - RINISnet
 - OTwolk
 - Suwinet
 - het AOD gedeelte binnen Gemnet

Buiten Diginetwerk vallen daarmee

- de overige VPN's van Haagse Ring
- Het Gemnet Non-overheids VPN met CUG en het leveranciers CUG

Grenzen van de services

Services vallen feitelijk niet binnen Diginetwerk. Ze zijn een verantwoordelijkheid van de betreffende beheerder. Er is ook nauwelijks sprake van harmonisatie in het kader van Diginetwerk. Er zijn alleen afspraken gemaakt over de connectiviteit tussen bepaalde services, zoals bijv tussen de DNS'en of tussen mailrelays.

3.10 Beheer

3.10.1 Inleiding

Diginetwerk bestaat uit diverse (typen) beheerdomeinen en objecten. Binnen de grenzen van Diginetwerk gaat het vooral over het beheer van de diverse koppelnetwerken (met hun services) en het beheer van het BasisKoppelNetwerk, vooral in hun onderlinge relatie zoals die speelt bij de ketens van netwerken en voorzieningen. In een bepaalde verbinding tussen een client bij organisatie A en een server bij organisatie B zullen zich diverse netwerken met verschillende beheerders bevinden.

Beheer van Diginetwerk kent globaal 2 niveaus:

- Het beheer van de individuele koppelnetwerken (incl. BKN)
- Het beheer van de keten van netwerken

Voor de architectuur van Diginetwerk is met name het ketenaspect van belang. Het beheer van de individuele koppelnetwerken is immers een zaak van de betreffende beheerders en voor bestaande netwerken al ingericht.

Diginetwerk moet zodanig opgezet en ingericht zijn dat beheerbaarheid gewaarborgd is. Dat betreft technische zaken zoals onderhoudbaarheid, effectieve mogelijkheden voor incidentmanagement (diagnose, monitoring en rapportages) en organisatorische zaken zoals verantwoordelijkheids-grenzen, afspraken/convenanten etc.

Tevens zijn er (meer strategische) beheertaken te onderkennen op het overall niveau van Diginetwerk. Dat richt zich o.a. op de gehele keten van alle gekoppelde netwerken. Daarvoor is een regietaak onderkend die o.a. verantwoordelijk is voor het governance model.

Deze complexe situatie vereist eenduidige verdeling van verantwoordelijkheden en bevoegdheden, afspraken over nauwe samenwerking, inzicht in elkaars contact- en netwerkgegevens (SLA's en DAP's), conform BiSL en ITIL.

De beheermaatregelen voor Diginetwerk besteden specifiek aandacht aan de noodzakelijke afspraken om adequaat te handelen in de ketens van netwerken. Dat beheer wordt in separate documenten behandeld.

De aangesloten organisatie heeft een contract met "zijn" koppelnetwerkbeheerder. Daarmee voldoen deze afspraken aan NORA principe AP 27.

De verdere uitwerking van deze afspraken valt buiten het bestek van deze architectuur.

In het kader van de beheerbaarheid zullen ook technische voorzieningen nodig zijn. De belangrijkste eisen aan de (technische) architectuur die gesteld worden vanuit beheer zijn:

- Goede scheiding van domeinen.
Dit wordt bereikt door de eis dat alle beheerde netwerken begrensd worden op laag 3. Daardoor kan iedere beheerder volledig verantwoordelijk zijn voor zijn eigen domein met eigen nummerplan (zie paragraaf 3.5).

- Eenduidige belegging van beheer van routeringen
Koppelnetswerken worden ook begrensd op laag 3 waardoor beheer van routeringstabellen niet op de randen plaatsvindt bij beheerders van bedrijfsnetwerken, maar bij de beheerders van de koppelnetswerken (zie paragraaf 3.5).
- Faciliteiten t.b.v. incident- en capaciteitsmanagement e.d.
Beheerders beschikken over faciliteiten om storingsdiagnose etc. te ondersteunen (zie paragraaf 3.3.1).
- Hoge beschikbaarheidseisen moeten beheerd (waargemaakt) kunnen worden.
Verbindingen etc. zijn als dienst met SLA's verkregen. Binnen de grenzen van Diginetwerk zijn er geen Single Points of Failure (SPoF's), dubbele componenten kennen automatische failover (zie paragraaf 3.5.2).

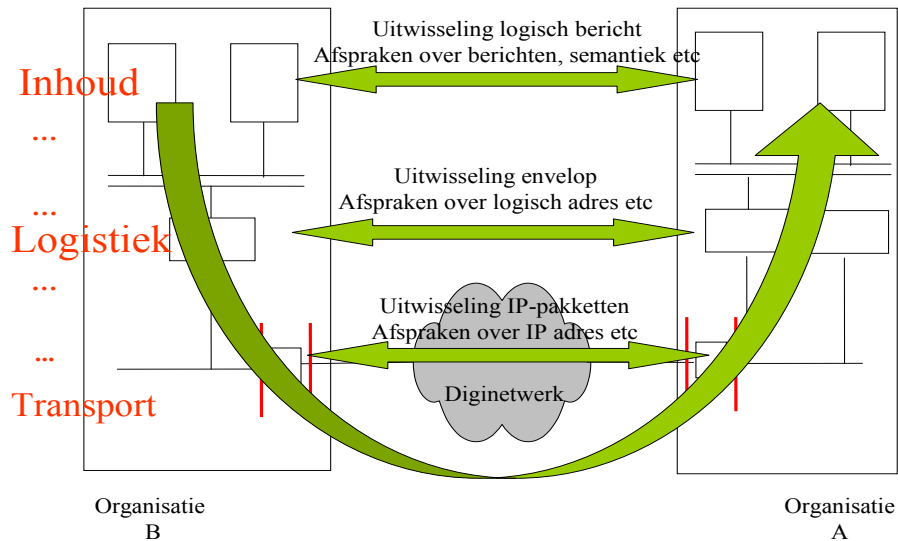
Deze eisen en maatregelen zijn in dit document eerder behandeld.

3.10.2 *Architectuur en Ontwerp aspecten bij Aansluiten*

Vanuit de architectuur van Diginetwerk, in samenhang met andere architectuurconcepten en -bouwstenen worden in deze paragraaf een aantal aspecten geschetst die relevant zijn bij het aansluiten van een organisatie op Diginetwerk.

Voor een organisatie die gebruik wil maken van Diginetwerk voor uitwisselingen in de eOverheid zijn eerst een aantal afbakeningen van belang:

1. Diginetwerk gaat alleen over de connectiviteit. Dat betekent dat de volgende afspraken geen betrekking hebben op diginetwerk
 - a. de inhoud en semantiek van berichten, resp. gebruik van een website
 - b. logistiek, bijv koppelvlakken van Digikoppeling resp. bereiken van een website (url)
2. Diginetwerk, dus connectiviteit, betreft in normale gevallen vooral het aansluiten van een organisatie op Diginetwerk, en mogelijk voor bepaalde aspecten het verbinden met een bepaalde service.



Figuur 16 Diginetwerk in de set uitwisselingsafspraken

Dit wordt toegelicht aan de hand van uitwisseling van berichten tussen organisatie A en B, geschetst in bovenstaande Figuur 16. Om uitwisseling te realiseren moeten afspraken gemaakt worden over de "Inhoud", berichten en semantiek etc. Die afspraken t.a.v. de uitwisseling van het logische bericht worden geïmplementeerd in applicaties in beide organisaties.

Om berichten uit te wisselen tussen de postkamers van beide organisaties moeten afspraken gemaakt worden over de logistiek, d.w.z. over de envelop van het bericht. Die worden geïmplementeerd in adapters resp. middleware software. Een belangrijk aspect van die logistieke afspraken betreft het logische adres van de services die gebruikt wordt, de url.

Pas in de onderste laag komt Diginetwerk aan bod.

De afspraken van Diginetwerk beschrijven hoe DNS-publicatie en -resolving plaatsvinden. Daarmee wordt de url (FQDN) omgezet in een destination IP-adres.

De organisatie die een IP-pakket naar dat Destination IP adres wil sturen (de service requester) dient zelf de eigen infrastructuur ingeregeld te hebben waardoor alle pakketten bedoeld voor IP-adressen van Diginetwerk gerouteerd worden naar de Diginetwerkaansluiting, en zorgen dat hun firewalls dat verkeer doorlaten.

Diginetwerk is – na oplevering van Diginetwerk – zodanig ingericht dat het betreffende pakket wordt afgeleverd bij de voordeur van de aanbieder, Organisatie A.

Organisatie A moet zijn infrastructuur zodanig hebben ingericht dat de betreffende stroom doorgelaten wordt door de firewall en wordt afgeleverd bij de juiste interne servers.

Wanneer organisaties zijn aangesloten op Diginetwerk hebben ze de beschikking gekregen over een aantal IP-adressen, die ze zelf moeten toewijzen aan services (publiceren DNS). Die toedeling is in principe niet interessant voor beheerders binnen Diginetwerk. Diginetwerk routeert een set IP-adressen naar een organisatie, en de organisatie is zelf verantwoordelijk voor het correct koppelen van adressen aan services en het publiceren in DNS.

Op dit moment zijn organisaties die met elkaar uitwisselen wel geïnteresseerd in elkaars IP-adressen i.v.m. firewall rules.

Mogelijk kan in de toekomst in veel gevallen afgezien worden van specifieke firewall rules per source/destination paren. Voor tweezijdig TLS beveiligde verbindingen zou volstaan kunnen worden met filteren op Diginetwerk reeksen op de firewall.

Alleen in geval van een storing (hetzij initieel bij inrichting van een verbinding, hetzij later tijdens operationeel gebruik) is het noodzakelijk om de Diginetwerk beheerders te laten zoeken op IP-adres.

Afhankelijk van de dienstverlening van het koppelnetwerk kan een organisatie zelf een deel van de diagnose doen m.b.v. ping en traceroute, dan wel daarvoor gebruik maken van de diensten van het koppelnetwerk.

I. BIJLAGE I NORA Normen IB

Citaat uit "NORA Normen Informatiebeveiliging ICT-voorzieningen" m.b.t. Zones.

Principe

ICT-voorzieningen zijn in zones ingedeeld.

Definitie

Een zone is een afgebakend netwerk van ICT-voorzieningen, waarbinnen gegevens vrijelijk kunnen worden uitgewisseld. Gegevensuitwisseling met andere zones verloopt via koppelvlakken.

Toelichting

Het primaire doel van zonering is isolatie van risico's, waardoor bedreigingen en incidenten in de ene zone niet doorwerken in een andere. Hierbij gaat het er niet alleen om de interne tegen de externe, onvertrouwde zone te beschermen, maar ook om interne zones, zoals bijvoorbeeld ontwikkeling, test, acceptatie en productie-omgevingen, van elkaar te scheiden.

Zonering maakt het voorts mogelijk om met verschillende beveiligingsniveau's binnen een infrastructuur te werken en informatiestromen en risicovolle beheercommando's te reguleren. Deze toegangbeperking is soms krachtiger dan toegangsbeveiliging via aanlogprocedures bij servers. Zonering maakt het netwerk overzichtelijker voor beheer en dat is tevens van belang voor beveiliging.

Elke zone kent dus andere risico's samenhangend met de diensten of ICT-voorzieningen die erin opgenomen zijn. Binnen zones kunnen met standaard maatregelen sub-zones worden ingericht als het risicoprofiel dat vereist, bijvoorbeeld om verschillende productieomgevingen uit elkaar te houden, die niet het zelfde beveiligingsniveau hebben. Externe netwerken worden in dit zoneringconcept ook als aparte zone gezien.

De controle op informatiestromen tussen zones wordt verzorgd door zogenaamde filterfuncties, die als aparte IB-functie worden gezien. Bij end-to-end beveiliging waarbij de berichten of documenten zelf beveiligd zijn, zal minder filtering noodzakelijk zijn, maar dat doet vooralsnog niets af aan het zoneringconcept.

Zonering heeft betrekking op het geheel van de ICT-voorzieningen

Motivering

Door zonering kunnen risico's worden geïsoleerd, waardoor bedreigingen en incidenten die optreden in de ene zone niet doorwerken in een andere zone.

Eisen te stellen aan zones

Doelstelling van de maatregel

Zones zijn als eenheid van beveiliging en beheer gedefinieerd.

Implementatierichtlijnen

- 1. Elke zone heeft een vastgesteld beveiligingsdoel.*
- 2. Elke zone wordt slechts beheerd onder verantwoordelijkheid van een beheerinstantie (m.u.v. onvertrouwde derden).*

3. Een zone heeft een gedefinieerd beveiligingsniveau, d.w.z. kent een gedefinieerd stelsel van samenhangende beveiligingmaatregelen.
4. De maatregelen van logische toegangsbeperking zijn van toepassing op alle ICT-voorzieningen in een zone.
5. Uitwisseling van gegevens tussen zones vindt uitsluitend plaats via een gedefinieerd koppelvlak.
6. Zones kunnen worden onderscheiden door gebruikmaking van routing van datastromen, verificatie van de bron- en de bestemmingsadressen (Code 11.4.7), door toepassing van verschillende protocollen, encryptietechnologie, partitionering van servers, maar ook door fysieke scheiding
7. Zonering wordt ingericht met voorzieningen, waarvan de functionaliteit is beperkt tot de strikt noodzakelijke (hardening van voorzieningen).
8. Bij elkaar behorende serverfuncties bevinden zich slechts in één zone.

Filtering

Principe

Op het koppelvlak tussen zones zijn filterfuncties gepositioneerd voor het gecontroleerd doorlaten van gegevens.

Definitie

Het doel van filtering is bescherming van zones tegen het doorlaten van Denial of Service attacks, indringers, ongewenste inhoud, virussen en informatie lekkage.

Toelichting

Filtering controleert in- en uitgaande gegevensstromen op locatie, vorm (protocol) of inhoud van gegevensstromen, afhankelijk van de aard van de stromen en zones. Filtering controleert geen identiteiten van individuele gebruikers.

De communicatie tussen twee zones wordt getoetst op ongewenst gedrag. Daarvoor wordt een elektronisch profiel vastgelegd van de zenders in de betrokken zones. Van het communicatiegedrag wordt elektronisch een 'reputatie score' vastgelegd, dat enerzijds wordt vergeleken met het beleidsregels voor doorlaten van communicatie en anderzijds met bekende patronen van ongewenste communicatie.

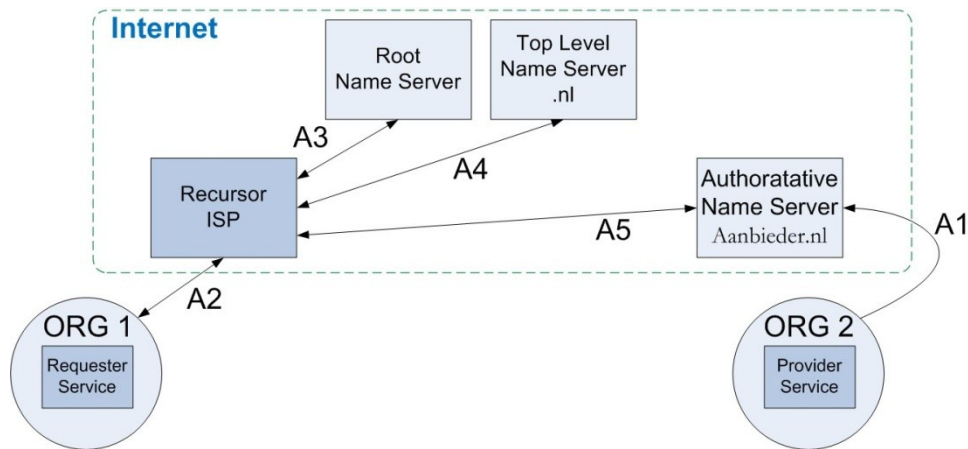
Motivering

Filterfuncties zijn onlosmakelijk verbonden aan het principe van zonering en ontleen daaraan ook hun motivatie.

II. Bijlage DNS

In deze bijlage worden enige relevante eigenschappen van DNS beschreven. Doel is om voldoende achtergrond te geven voor de beschreven oplossing van Diginetwerk, resp. om de gehanteerde terminologie eenduidig te definiëren.

De basis van DNS werking is geschetst in onderstaande figuur.



Organisatie ORG2 publiceert zijn service, bijv met FQDN service1.aanbieder.nl, in de DNS op internet die authoritative is voor zijn domein "aanbieder.nl". Deze stap is aangegeven met A1. Als organisatie ORG1 die service wil gebruiken zal ORG1 de FQDN willen resoluten naar het betreffende IPadres via de internet recursive DNS (recursor) bijvoorbeeld van zijn ISP, aangegeven met A2. Die recursor doet vervolgens de resolving via het normale internet DNS-stelsel (A3-A5). De resolver gaat eerst bij de Root Name Server opvragen waar de Top Level Name Server voor het nl domein zich bevindt. Via die DNS wordt opgevraagd waar de DNS voor het domein aanbieder.nl zich bevindt; in die DNS wordt het IPadres gevonden voor service.aanbieder.nl. De diverse stappen worden gecached.

III. BIJLAGE Classificering uit IB-plan Logius

Classificering en beheer van informatiesystemen

Doelstelling van dit onderdeel is het handhaven van een adequate bescherming van bedrijfsmiddelen. Alle belangrijke bedrijfsmiddelen dienen een eigenaar te krijgen die verantwoordelijk is voor het handhaven van de juiste beveiligingsmaatregelen. Het bepalen van de verantwoordelijkheden voor bedrijfsmiddelen draagt ertoe bij dat deze op de juiste manier beveiligd blijven. De verantwoordelijkheid voor het implementeren van de beveiligingsmaatregelen mag worden gedelegeerd. De eigenaar blijft echter verantwoordelijk voor het bedrijfsmiddel.

- **Algemene maatregelen**

1. Elke voorziening kent een eigenaar. Deze eigenaar is eindverantwoordelijk voor de voorziening.
2. Per voorziening is er een overzicht van de logische en fysieke componenten waaruit de voorziening is samengesteld, inclusief koppelvlakken met de buitenwereld – i.e. een architectuurplaat.
3. Elke voorziening kent een classificatie die gemaakt is op basis van onderstaand informatiebeveiliging classificatieschema:

Kwaliteits-aspect	Waardering			
	Niveau 0	Niveau 1	Niveau 2	Niveau 3
Beveiliging classificatie (algemeen)	Beveiliging is geen criterium voor de organisatie.	Een zekere mate van beveiliging wordt op prijs gesteld.	Beveiliging is absoluut nodig gezien de belangen van de organisatie.	Beveiliging is primair criterium voor de organisatie.
Beschikbaarheid	Onnodig. Er hoeven geen garanties te worden behaald.	Noodzakelijk. Een enkele keer uitval is aanvaardbaar.	Wezenlijk. Nauwelijks uitval gedurende de openingstijd.	Onmisbaar. Slechts in uitzonderlijke gevallen niet operationeel.
Exclusiviteit	Openbaar. Gegevens hoeven niet te worden afgeschermd.	Afgeschermd. Gegevens alleen ter inzage voor een bepaalde groep.	Cruciaal. Gegevens alleen toegankelijk voor direct betrokkenen.	Dwingend. Bedrijfsbelangen worden ernstig geschaad als ongeautoriseerden toegang krijgen.
Integriteit	Passief. Geen extra integriteitbescherming.	Actief. Bedrijfsproces tolereert enkele fouten.	Detecteerbaar. Een zeer beperkt aantal fouten is toegestaan.	Onontbeerlijk. Bedrijfsproces eist foutloze informatie.

Tabel 1

De classificatie van de voorzieningen wordt jaarlijks herzien en tevens als er veranderingen – bijvoorbeeld uitbreidingen – zijn inzake de voorziening. De consequenties van een verandering in classificatie – i.e. aanvullende informatiebeveiligingsmaatregelen – worden zo spoedig mogelijk geïmplementeerd.

4. Informatie – zowel digitaal als afgedrukt – wordt voorzien van een exclusiviteitwaardering, zoals beschreven in het informatiebeveiliging classificatieschema. De relatie van deze exclusiviteitwaardering met classificaties uit het VIR-BI en WBP (op basis van Achtergrondstudies en Verkenning 23) komen bij benadering met elkaar overeen zoals weergegeven in de volgende tabel.

Exclusiviteitwaarderin g	VIR-BI Classificatie	WBP Classificatie
Openbaar		Risicoklasse 0
Afgeschermd		Risicoklasse 1
Cruciaal	Dep. Vertrouwelijk	Risicoklasse 2
Dwingend	Stg. Confidentieel	Risicoklasse 3
	Stg. Geheim / Zeer Geheim	

Tabel 2