

Beleidsonderzoek modemkeuze

*Analyse consultatiereacties betreffende
technische implicaties vrije modemkeuze*

RAPPORT

Rapport uitgebracht aan
Ministerie van Economische Zaken en Klimaat
DGTM

Hilversum, 16-10-2018

Inhoudsopgave

1	Introductie.....	5
1.1	Aanleiding en context.....	5
1.2	Doel van het onderzoek.....	5
1.3	Methodiek.....	6
1.4	Leeswijzer	7
1.5	Begrippenlijst.....	8
2	Beleidsachtergrond	11
2.1	Richtlijn 2008/63/EG.....	11
2.2	Besluit Eindapparaten (dec 2016)	12
2.3	Concept Beleidsregel Netwerkaansluitpunt (dec 2017).....	13
2.4	De praktijk van het beleid.....	14
2.5	Ontwikkelingen in Europa ten aanzien van veiligheid & IoT	15
3	Technische achtergrond.....	18
3.1	Analytisch framework voor de analyse van het netwerk.....	18
3.2	Horizontale netwerk analyse: indeling naar netwerktopologie	18
3.3	Verticale netwerkanalyse: het functionele lagenmodel.....	21
3.4	Bruikbaarheid modellen bij validatie.....	23
4	Inventarisatie en groepering issues.....	25
4.1	Overzicht en achtergrond reacties.....	25
4.2	Netwerkbeheer.....	27
4.3	Veiligheid	27
4.4	Diensten.....	28
4.5	Eigen netwerk en apparatuur	28
4.6	Definities en consistentie van regelgeving.....	29
4.7	Standaarden netwerkaansluiting.....	29
4.8	Overige opvallende reacties	30
5	Analyse: Validatie technische argumenten	31
5.1	Issues rond impact op Operator Netwerk.....	31
5.2	Issues rond impact op Veiligheid	38
5.3	Issues rond impact op diensten	41
5.4	Issues rond impact op eigen netwerk en eigen apparatuur.....	50
5.5	Issues met betrekking tot standaarden netwerkaansluiting	51
6	Analyse beheersbaarheid	54

7	Conclusie, impact en aandachtspunten	57
7.1	Doel.....	57
7.2	Aanpak.....	57
7.3	Conclusie.....	57
	Literatuurlijst.....	61
Annex A	Samenvatting consultatiereacties	62
A.1	Netwerktogang, operator netwerk	62
A.2	Veiligheid	63
A.3	Diensten.....	64
A.4	Eigen netwerk en apparatuur	65
A.5	Definities en consistentie van regelgeving.....	65
A.6	Standaarden netwerkaansluiting.....	66
A.7	Overige opvallende reacties	67
Annex B	Overzicht openbare reacties	69
Annex C	Overzicht niet openbare reacties	73
Annex D	Overzicht achtergrondinformatie	74
Annex E	Interviews n.a.v. het conceptrapport in het kader hoor-wederhoor	83
E.1	Inleiding	83
E.2	Interviewverslag CAIW en NLConnect.....	87
E.3	Interviewverslag Eurofiber	91
E.4	Interviewverslag KPN	96
E.5	Interviewverslag Tele2	101
E.6	Interviewverslag T-Mobile.....	106
E.7	Interviewverslag VodafoneZiggo.....	110
E.8	Interviewverslag VTKE	119

1 Introductie

1.1 Aanleiding en context

Op 21 december 2016 is het Besluit Eindapparaten gepubliceerd [3]. Het ministerie van Economische Zaken en Klimaat (EZK) is voornemens, mede met het oog op vrije keuze van eindapparaten, in een beleidsregel de locatie van het netwerkaansluitpunt te verduidelijken en daarbij duidelijk te maken dat nagenoeg alle apparatuur die op het netwerkaansluitpunt van het openbare netwerk worden aangesloten (waaronder modems ¹of modem/routers) niet behoren tot een openbaar elektronisch communicatienetwerk. Deze voorgenomen beleidsregel 'Vrije Modemkeuze' is inmiddels geconsulteerd.

In het kader van het Besluit Eindapparaten (2016) en de voorziene beleidsregel heeft EZK daarnaast gesprekken met diverse stakeholders gevoerd. Hierbij hebben partijen uit de telecomwereld en sommige gebruikers een aantal zorgpunten onder de aandacht gebracht rond veiligheid van netwerken, continuïteit en kwaliteit van dienstverlening.²

1.2 Doel van het onderzoek

Het doel van het onderzoek was om op basis van de consultatieresultaten een inschatting van mogelijke risico's te verkrijgen in puur technische zin (wat kan er potentieel misgaan, gegeven het huidige niveau van beveiliging door fabrikanten bijvoorbeeld). Deze risico's werden vervolgens gezien in de *context* van:

- 1) mogelijke *operationele, technische en contractuele maatregelen* die *netwerkaanbieders* kunnen nemen om de desbetreffende veiligheidsrisico's te adresseren;
- 2) mogelijke *ontwikkeling ten aanzien van niveau van beveiliging van eindapparaten* door *fabrikanten*; en/of verkopers/verstrekkers
- 3) *verantwoordelijkheden* die bij *eindgebruikers* kunnen worden belegd voor de *beveiliging van private netwerken*.

Dit rapport heeft als uiteindelijk doel een handvat te bieden om de specifieke argumenten uit de consultatie van de beleidsregel die betrekking hebben op veiligheidsrisico's, adequaat te kunnen beoordelen en mee te nemen in een uiteindelijk besluit.

¹ In dit rapport wordt er vanuit gegaan dat de beleidsregel impliceert dat alles achter het netwerkaansluitpunt vrij gekozen kan worden door de consument. Dit betreft niet alleen het apparaat dat signalen moduleert en demoduleert op de kabel, de zogenaamde modem of ook wel NTU genoemd, maar ook de daar veelal mee geïntegreerde router, welke verkeer naar binnen of buiten het thuisnetwerk geleidt en veelal ook network address translation, dhcp en andere diensten levert. Vandaar dat de termen modem, NTU en modem/router afhankelijk van de context gebruikt worden. Een router in bridge mode functioneert als een modem.

² Indien commentaar vanuit de consultatie geciteerd wordt, dan wordt er gebruik gemaakt van *cursief* met hierachter een code [XXX] welke in de Annex X staan.

Scope

Bij de inschatting van de genoemde gevolgen is waar mogelijk zowel *naar de korte als langere termijn* (2020 e.v.) gekeken. Het onderzoek richtte zich op argumenten die:

- in de consultatie naar voren kwamen; en
- betrekking hebben op technische en operationele aspecten; en
- als gevolg van de beleidsregel een risico vormen voor de veiligheid, werking en continuïteit van:
 - de openbare netwerken; en van
 - private netwerken (thuisnetwerken en klein zakelijk); en
 - apparaten die daarop zijn aangesloten.

Het onderzoek richt zich expliciet niet op de interpretatie van wet- en regelgeving. Het gaat uit van de definities en uitleg zoals deze door het Ministerie gegeven zijn.

Het onderzoek richt zich niet op duiding van juridische aspecten en samenhang met andere regelgeving, Wel zijn op een aantal plaatsen mogelijke issues in dit kader kwalitatief benoemd.

Het onderzoek richt zich alleen globaal op organisatorische aspecten, deze werden in de consultatiereacties vrijwel alleen in kwalitatieve zin benoemd. Kwantitatief onderzoek naar kostenaspecten en organisatorische impact was geen deel van dit onderzoek.

Doordat het onderzoek zich primair richt op issues die in de consultatie naar voren kwamen, er is geen uitputtende inventarisatie gedaan van andere mogelijke issues. Wel zijn een aantal additionele issues benoemd waar deze bij de beschouwing van de in de consultatie genoemde issues relevant zijn.

1.3 Methodiek

Stratix volgde in dit onderzoek de methodiek en tweedeling die is voorgesteld door EZK:

- A. Validatie van de sec technische argumenten die in de consultatie naar voren kunnen komen als mogelijke bedreiging van de veiligheid van de openbare netwerk en private netwerken
- B. Validatie van de onder A naar voren gekomen overige argumenten, tegen de achtergrond van het bredere beleidskader

De argumenten werden daarbij geanalyseerd in het kader van mogelijkheden die netwerkaanbieders hebben om veiligheidsrisico's beheersbaar te maken, gegeven:

- de *verplichtingen* die op hen rusten in het kader van het *Besluit eindapparaten*;
- de *voorzien*e beleidsregel en andere bestaande relevante regelgeving;
- de *verantwoordelijkheden* die bij eindgebruikers kunnen worden belegd voor de beveiliging van private netwerken; en
- *het huidige en te verwachten niveau van beveiliging van eindapparaten door fabrikanten mede op basis van toekomstige regelgeving.*

Aanvullende achtergrondinformatie

Naast de verschillende consultatiereacties, die ingaan op zowel de huidige situatie en de huidige regelgeving als de beoogde regelgeving en de situatie die daarmee mogelijk ontstaat, is er voor dit onderzoek gebruik gemaakt van achtergrondinformatie uit verschillende bronnen.

- Relevante Europese, Duitse en Nederlandse wetten en artikelen over de interpretatie ervan
- Opiniëartikelen over de situatie in Duitsland³ en de impact van de nieuwe wet in Duitsland
- Onderzoeken met betrekking tot de functie van modems en demarcatie van operator netwerken

In Annex D is een overzicht gegeven van de voor dit onderzoek gebruikte achtergrondinformatie.

Op initiatief van de opdrachtgever is het draft rapport voorgelegd aan een aantal door opdrachtgever geselecteerde partijen in het kader van hoor en wederhoor, en is aan die partijen gelegenheid gegeven tot een reactie in de vorm van een interview. De interviewverslagen zijn te vinden in Annex E.

1.4 Leeswijzer

In hoofdstuk 2 schetsen we het bredere beleidskader van het Besluit Eindapparaten en de voorgenomen beleidsregel 'vrije modemkeuze' die onderwerp was van de consultatie. Hierbij wordt de context geschetst van relevante landelijke en Europese regelgeving. In overleg met het Ministerie van Economische Zaken is er besloten om in dit document geen verdere uitleg of interpretatie te geven van de regelgeving. In de beoordeling van de argumenten voor en tegen een vrije modemkeuze wordt er vanuit gegaan dat alle apparaten die genoemd worden onder deze vrije keuze vallen.

Hoofdstuk 3 gaat in op de technische achtergrond van het elektronische communicatienetwerk. De horizontale en verticale opdeling van het netwerk helpt ons bij de analyse van de verschillende argumenten van de consultatie. Bovendien grijpen we terug naar deze opdelingen bij de analyse en validatie (hoofdstuk 5).

Hoofdstuk 4 geeft een inventarisatie van zowel de argumenten in de consultatie (verdeeld in categorieën), als de documenten die in de argumentatie en door de beleidsmaker gebruikt zijn.

In hoofdstuk 5 worden de issues en hun effecten op basis van technologische argumenten geanalyseerd en gevalideerd.

Na de validatie vanuit technisch perspectief (H5), geven we in hoofdstuk 6 een verdere analyse van de beheersbaarheid van de risico's en mogelijke mitigatiemaatregelen.

We sluiten het rapport af met een aantal algemene conclusies in hoofdstuk 7.

³ In Duitsland is in 2016 wetgeving ingevoerd die vrije modemkeuze mogelijk maakt

1.5 Begrippenlijst

NTU	Network Termination Unit: het passieve of actieve apparaat dat het demarcatiepunt markeert tussen operator- en thuisnetwerk.
DSLAM	Digital subscriber line access multiplexer. Apparaat dat digitale (DSL) communicatie over een aantal koper(telefoon)lijnen verbindt met een glasvezel backbone netwerk. Bevindt zich meestal in oude telefooncentrales.
DOCSIS	Data Over Cable Service Interface Specification. Een standaard om data-transport (en dus internettoegang) over kabelnetwerken mogelijk te maken. Er zijn verschillende versies, tegenwoordig is DOCSIS-3 gebruikelijk.
VDSL	Very-high-bit-rate digital subscriber line. DSL is een standaard om data-transport (en dus internettoegang) over koper(telefoon)netwerken mogelijk te maken. Er zijn verschillende versies Tegenwoordig is VDSL-2 gebruikelijk.
PSTN	Public switched telephone network. Het traditionele telefonienetwerk.
FTU	Fiber Termination Unit: eindapparaat voor glasvezelverbindingen in de meterkast.
NAT	Network Address Translation: vertaling van interne IP adressen in een thuis- of bedrijfsadres naar openbare IP adressen (waarvan vaak veel minder beschikbaar zijn).
DRM	Digital Rights Management: technieken voor het beheren van de auteursrechten van digitale content zoals muziek of films.
TCP-IP	Transfer Control Protocol – Internet Protocol, een protocol boven op het basis Internet Protocol (IP) dat zorgdraagt dat informatie tussen zender en ontvanger zonder informatieverlies en in de juiste volgorde wordt ontvangen.
STB	Set Top Box, verzamelnaam voor apparaten die gebruikt worden om TV en/of radiodiensten af te leveren en aan te sluiten op Tv's en audioversterkers.
OSI model	Open Systems Interconnection model, conceptueel model om lagen binnen een telecomdienst te onderscheiden, gedefinieerd door de ISO
ISO	International Organization for Standardization
MAC adres	media access control address. Ingebakken hardware adres van apparaten dat lokaal wordt uitgewisseld als netwerk adres in Ethernet en Wifi netwerken. Hierdoor is lokaal identificatie en dus communicatie mogelijk, ook voordat er IP adressen zijn toegekend.
SIP	Session Initiation Protocol. Een protocol om media sessies (zoals telefonie, videobellen, conference calls en dergelijke) op te zetten, te veranderen en af te breken. Wordt tegenwoordig over IP vaak gebruikt als vervanging van of aanvulling op klassieke telefonie protocollen.

FttH	Fiber tot he Home: glasvezel als access technologie tot in de meterkast van woonhuizen, appartementen e.d. van de consument
ISDN	Integrated Services Digital Network. Set van standaarden als aanvulling op de klassieke telefoniefuncties, die naast spraak ook data en aanvullende diensten ondersteunen.
PPP en PPPoE	Point to Point protocol over Ethernet. Een ppp protocol wordt gebruikt om initieel een Ethernet sessie op te zetten. Dit principe wordt in diverse vaste en mobiele omgevingen gebruikt ⁴
GPON	Gigabit capable Passive Optical Network. Glasvezelnetwerkstructuur waarbij verschillende eindpunten (bijvoorbeeld huishoudens) vanaf een centraal punt (bijvoorbeeld een centrale) worden aangesloten via 1 fiber die zich onderweg splitst in meerdere fibers, zonder dat hier actieve apparatuur voor wordt gebruikt.
ISP	Internet Service Provider: de aanbieder van internettoegang.
GSM	Global System for Mobile communications, een ETSI standaard voor mobiele communicatie (ooit begonnen als 'Groupe Spécial Mobile') die zou uitgroeien tot wereldwijde standaard voor de 2 ^e generatie mobiele communicatie (2G) en de basis legde voor ontwikkelingen als GPRS (2.5G) UMTS (3G), LTE (3.5G) LTE Advanced en LTE Advanced Pro (4.5G) en 5G.
UMTS, LTE, 4G	Zie GSM
AP	(WiFi) Access Point
IPTV	IP televisie, televisie over een IP netwerk
DNS	Domain Name Server, server die domeinnamen in een web adres zoals in een URL vertaalt naar een IP adres.
URL	Uniform Resource Locator, combinatie van aanduiding van een protocol (bijvoorbeeld http) , een web adres (bijvoorbeeld www.voorbeeld.nl) en een file naam (bijvoorbeeld index.html)
HTML	protocol om webpagina's te maken
HFC	Hybrid Fiber Coax, een netwerk met glasvezel in de kern van het netwerk en coax voor de verbindingen met huishoudens
(A)DSL, VDSL	(Asynchronous) Digital Subscriber Line, protocol om koperen telefoonverbindingen geschikt te maken voor tweeweg datatransport. Varianten en opvolgers: ADSL, ADSL2, VDSL,

⁴ https://www.researchgate.net/publication/220440493_Quality_of_Service_for_SIP_Sessions_in_3GPP-based_Networks

FTC	Federal Trade Commission, Amerikaanse overheidsorganisatie voor bescherming van consumentenbelangen
NITRO	optie op de Broadcom chips voor ADSL+ verbindingen waarmee snelheden tot 30 Mbps bereikt kunnen worden tussen huishouden en straatkast, mits beide deze chipset gebruiken.'
MP-TCP	Multipath TCP, variant van TCP protocol waarmee één dataflow via verschillende paden kan worden verstuurd, als een rivier die zich in tweeën splitst en later weer bij elkaar komt.
TCP	Transfer Control Protocol, samen met IP de basis voor internet. Met TCP wordt een IP verbinding betrouwbaar omdat de verstuurd pakketten in de juiste volgorde en met ontvangstbevestiging worden afgeleverd bij de ontvanger.
NTU	Network Termination Unit
FTU	Fiber Termination Unit
VULA	Virtual Unbundled Local access, andere operators kunnen daarbij gebruik maken van het access netwerk van een operator om daarover diensten aan te bieden.

2 Beleidsachtergrond

Dit hoofdstuk bespreekt de achtergrond ten aanzien van de nieuwe beleidsregels van Economische Zaken en Klimaat en plaatst ze binnen de juridische context.

2.1 Richtlijn 2008/63/EG

Al in 1988 werden er in de Europese Gemeenschap afspraken gemaakt over mededinging op de markten van telecommunicatie-eindapparatuur [6]. Deze richtlijn is in 2008 vervangen door Richtlijn 2008/63/EG betreffende de mededinging op de markten van telecommunicatie-eindapparatuur [7]. 2008/63EG geeft een aantal overwegingen ten aanzien van de markten van telecommunicatie-eindapparatuur welke relevant zijn voor de context van dit onderzoek. In onderstaand kader staan enkele van de voor dit onderzoek meest relevante overwegingen en artikelen uit de richtlijn:

3. Technische en economische ontwikkelingen hebben de lidstaten ertoe gebracht het stelsel van bijzondere of uitsluitende rechten op telecommunicatiegebied te herzien. Met name de snelle groei van de verschillende typen eindapparatuur en van de vele gebruiksmogelijkheden ervan maakt het noodzakelijk dat de gebruikers een vrije keuze uit deze typen wordt geboden zodat zij ten volle van de technologische vooruitgang op dit terrein kunnen profiteren.

10. Willen de gebruikers het eindapparaat van hun keuze kunnen gebruiken, dan is het nodig de kenmerken van de interface van het openbaar net waaraan het eindapparaat moet worden aangesloten, te kennen en doorzichtig te maken. De lidstaten moeten zich ervan vergewissen dat de eigenschappen ervan worden gepubliceerd en de interface van het openbaar net voor de gebruiker toegankelijk wordt gemaakt.

11. Het is voor een afzet van eindapparatuur nodig dat de producenten weten aan welke technische specificaties hun producten moeten voldoen. De lidstaten moeten er zorg voor dragen dat deze specificaties worden geformaliseerd en bekendgemaakt, en deze op grond van Richtlijn 98/34/EG van het Europees Parlement en de Raad van 22 juni 1998 betreffende een informatieprocedure op het gebied van normen en technische voorschriften en regels betreffende de diensten van de informatiemaatschappij [\(4\)](#) in ontwerp aanmelden bij de Commissie. [...]

In deze richtlijn wordt verstaan onder:

1. „eindapparatuur”: a) de apparaten die voor overbrenging, verwerking of ontvangst van informatie direct of indirect op de interface van een openbaar telecommunicatienet zijn aangesloten; in beide gevallen, direct of indirect, kan de aansluiting geschieden per draad, per optische vezel of via elektromagnetische golven; een aansluiting is indirect wanneer een apparaat geplaatst is tussen het eindapparaat en de interface van het net;

Artikel 4 De lidstaten zien erop toe dat de nieuwe interfaces van het openbare net aan de gebruiker zelf de mogelijkheid bieden eindapparatuur aan te sluiten en dat de fysieke eigenschappen van die interfaces door de exploitanten van openbare telecommunicatienetten worden gepubliceerd.

Uit de Richtlijn en haar uitleg volgt dat een aansluiting direct of indirect kan zijn. Indirect is wanneer er nog een apparaat geplaatst is tussen het eindapparaat en de interface van het net. Wel stelt artikel 4 dat nieuwe interfaces van het openbare net aan de gebruiker zelf de

mogelijkheid bieden eindapparatuur aan te sluiten. Ook moeten de exploitanten van openbare telecommunicatienetten de specificaties van de interfaces publiceren.

2.2 Besluit Eindapparaten (dec 2016)

In de Nederlandse wet is de Richtlijn vertaald in het Besluit Eindapparaten [3]. De definitie van eindapparaten is in de praktijk gelijk aan die van de Richtlijn. Het besluit vult de Richtlijn verder in door in Artikel 2 te stellen: *"Een aanbieder van een openbaar telecommunicatienetwerk publiceert de technische specificaties van de netwerkaansluitpunten op genoegzame wijze op de eigen internetpagina, voordat via deze netwerkaansluitpunten diensten aan het publiek beschikbaar worden gesteld."* De toelichting zegt dat *"de informatie, bijvoorbeeld wanneer deze gebruikersgebonden is, kan uiteraard tevens worden verstrekt via gerichte communicatie met eindgebruikers bijvoorbeeld in schriftelijke vorm bij het afsluiten van contracten. De bedoelde informatie en de wijze van bekendmaking is van belang voor aanbieders van eindapparaten om deze apparatuur te kunnen ontwikkelen, en waar van toepassing ook voor gebruikers, om de werking van in gebruik zijnde apparatuur aan te passen aan gewijzigde specificaties van netwerkaansluitpunten"*. Voor dit onderzoek is dit van belang omdat de publicatieplicht in een aantal reacties wordt aangehaald. Daarbij is het van belang omdat de door de aanbieders gepubliceerde technische specificaties in dit onderzoek gebruikt kunnen worden om de opmerkingen uit de reacties op de consultatie te verifiëren. In de reacties staan opmerkingen over technische interfaces en mogelijkheden en onmogelijkheden om zelf apparatuur aan te sluiten. De praktijk laat overigens zien dat niet alle aanbieders deze specificaties al publiceren.

In artikel 3 van het Besluit wordt gezegd *"Een aanbieder van een openbaar telecommunicatienetwerk zorgt er voor dat eindapparaten die voldoen aan de bij of krachtens het Besluit elektromagnetische compatibiliteit 2016 onderscheidenlijk het Besluit radioapparaten 2016 gestelde eisen, op daartoe geschikte netwerkaansluitpunten kunnen worden aangesloten en kunnen blijven worden gebruikt."* De uitleg hierbij is dat: *"Deze toegangsverplichting ziet op het in gebruik nemen van en het gebruik van eindapparatuur op een openbaar telecommunicatienetwerk. In het kader van deze verplichting mogen door een aanbieder van een openbaar telecommunicatienetwerk geen belemmeringen worden opgeworpen voor het afnemen van diensten door eindgebruikers met gebruik van eindapparaten die zijn geleverd door derde partijen. Uiteraard moeten die eindapparaten wel geschikt zijn om op het netwerk van die aanbieder te kunnen worden aangesloten. Of dit het geval is hangt af van het doelgebruik en de daarbij horende specificaties van het eindapparaat, die zijn af te leiden uit de door de fabrikant opgestelde documentatie voor het eindapparaat. Zo moet een modem dat bedoeld is voor aansluiting op een netwerk die een DOCSIS standaard ondersteunt aangesloten kunnen worden op alle netwerken die deze standaard toepassen."*

De uitleg maakt ook duidelijk dat deze verplichting verder gaat dan het stellen dat het netwerk het apparaat van de eindgebruiker dat geschikt is voor een bepaalde standaard moet ondersteunen als het netwerk deze standaard toepast. De aanbieder moet ook meewerken met het uitleggen hoe gebruikersnamen en wachtwoorden verwerkt worden en dient ook karakteristieken van het apparaat van de eindgebruiker te kunnen registreren, zoals het MAC-adres. De uitleg zegt hierover: *"De toegangsverplichting heeft een ruimere werking dan het fysiek kunnen aansluiten van eindapparaten. Zo zullen, al dan niet op verzoek van de eindgebruiker, ook technische en administratieve parameters voor zover deze niet vallen onder de in artikel 2*

genoemde technische specificaties, aan de eindgebruiker bekend moeten worden gemaakt. Dit geldt bijvoorbeeld voor gegevens om instellingen van eindapparaten te kunnen inzien of beheren, zoals gebruikersnamen en wachtwoorden, indien dat nodig is om andere eindapparaten direct of indirect aan te kunnen sluiten op een door een telecomaandbieder geleverd eindapparaat. Waar nodig zal de aanbieder ook zelf handelingen moeten verrichten om eindapparaten die toegang te verlenen. Daar kan het mede gaan om het verlenen van beveiligde toegang tot een netwerk via het gebruik van hardware-identifiers van eindapparaten. In de praktijk kan het bijvoorbeeld voorkomen dat een zogenaamd MAC-adres dat een modem identificeert moet worden ingevoerd in het netwerk van de aanbieder teneinde een (beveiligde) toegang tot het netwerk te realiseren.”

2.3 Concept Beleidsregel Netwerkaansluitpunt (dec 2017)

De Beleidsregel Netwerkaansluitpunt welke ter consultatie gelegd is, definieert de term netwerkaansluitpunt. Deze definitie moet verduidelijkt worden, omdat volgens het Ministerie *"Aanbieders van met name vaste netwerken met een bedrade aansluiting op de locatie van de eindgebruiker, zoals een koper- of glasaansluiting, zijn in toenemende mate bepaalde functionaliteiten van op deze netwerken aangesloten (radio)apparaten gaan beheren die zich op de fysieke (thuis)locatie van de abonnee bevinden."* [...] *"Het gaat in concreto om modems, combinaties van modem/router en televisiedecoders die noodzakelijk zijn voor het gebruik van elektronische communicatiediensten. Deze (radio)apparaten worden doorgaans meegeleverd bij het sluiten van een abonnement."* Even verderop legt ze uit dat de onduidelijkheid is ontstaan omdat: *"De bovengenoemde praktijk waarbij door telecomaandbieders geselecteerde (radio)apparaten moeten worden gebruikt bij een abonnement op een elektronische communicatiedienst staat op gespannen voet met de doelstelling van richtlijn 2008/63/EG. Het gaat immers om veelgebruikte basisapparaten waarvoor een breed marktaanbod bestaat. Dit marktaanbod wordt gedreven door de brede standaardisatie van netwerkprotocollen zoals VDSL en DOCSIS. Met deze achtergrond is het voor een effectieve implementatie van richtlijn 2008/63/EG van belang dat de genoemde apparaten als eindapparaten worden beschouwd zoals bedoeld in deze richtlijn. De positie van het netwerkaansluitpunt, dat de grens vormt tussen het openbare netwerk en eindapparaten, is daarvoor bepalend."*

Het netwerkaansluitpunt wordt in het besluit voor vaste netwerken beperkt tot die plek in huis waar een passieve aansluiting, zonder eigen stroomvoorziening, zich bevindt. De toelichting zegt: *"Samenvattend en kijkend naar de huidige praktijk bij bekabelde (coax-, koper-, glas)netwerken, ligt het netwerkaansluitpunt in deze gevallen direct na de eerste passieve schakeling of passief signaalfilter (splitter) op de locatie van de eindgebruiker. Deze apparatuur is onderdeel van de infrastructuur van het openbare elektronische communicatienetwerk. Zij wordt gekenmerkt door onafhankelijkheid van de feitelijke levering van een openbare elektronische communicatiedienst en is, in tegenstelling tot een eindapparaat, standaard aanwezig op de locatie van de mogelijke abonnee, ook als deze geen diensten afneemt via het openbare elektronische communicatienetwerk. In de praktijk wordt een dergelijk (radio)apparaat aangeduid met bijvoorbeeld "Abonnee Overname Punt"."*

Voor dit rapport is het dus van belang om te beoordelen hoe de reacties op de consultatie in lijn zijn met het Besluit Eindapparaten en in hoeverre zij valide argumenten voor of tegen de nadere definiëring uit de beleidsregel geven. Het uiteindelijk doel achter de beleidsregel is het verduidelijken van de door de Telecommunicatiewet in samenhang met het Besluit

Eindapparaten geboden mogelijkheden voor eindgebruikers om hun eigen apparatuur aan te sluiten op het netwerk, en de daarmee samenhangende verplichtingen voor aanbieders van netwerktoegang, apparatuurfabrikanten en eindgebruikers.

2.4 De praktijk van het beleid

Gezien de Richtlijn en het Besluit mag van de aanbieder verwacht worden dat *de technische specificaties van de netwerkaansluitpunten op genoegzame wijze op de eigen internetpagina gepubliceerd worden, voordat via deze netwerkaansluitpunten diensten aan het publiek beschikbaar worden gesteld*. In de praktijk blijkt dit veelal niet het geval. Er is wel informatie beschikbaar, maar vaak alleen via de fora van de aanbieders en andere online discussiegroepen en -pagina's. De aanbieders nemen soms deel aan deze discussies, maar vaker zijn het de eindgebruikers die elkaar helpen om apparaten verbonden te krijgen. De wijze van invulling verschilt per aanbieder:

- KPN publiceert geen gegevens. Klanten die een eigen modem willen aansluiten kunnen gegevens vinden via de site netwerkje.com, de fora van KPN en discussiefora als die van Tweakers.net.
- Telfort en XS4All zijn werkmaatschappijen van KPN, waarbij Telfort dezelfde apparatuur en infrastructuur als het hoofdmerk KPN gebruikt en XS4All voor het grootste deel dezelfde techniek gebruikt. Zij publiceren beide de gegevens op hun website⁵. Telfort (zie figuur) beperkt zich tot de gegevens van de internetverbinding en niet van de telefonie. XS4All geeft de gegevens van de telefonie wel en geeft zelfs iets van een handleiding.
- VodafoneZiggo klanten kunnen in het geheel geen gebruik maken van eigen modems. Zij kunnen wel een modem in bridge modus plaatsen.
- Tele2 gebruikers ontvangen geen instellingen en zullen ook een gebruikersnaam/wachtwoord uit de geleverde modem moeten halen om de eigen modem te authenticeren.⁶
- Caiway geeft haar klanten een glasvezelmodem, waarachter zij een eigen router kunnen zetten.
- T-Mobile geeft haar klanten geen gegevens en ondersteuning. De telefonie-instellingen zijn afgeschermd, maar het is sommige gebruikers wel gelukt om internettoegang met eigen modem te realiseren⁷.
- Een aantal kleinere aanbieders ondersteunt een eigen modem van gebruikers⁸ en/of het plaatsen van een eigen router.

⁵ <https://www.telfort.nl/persoonlijk/service/netwerkinstellingen-met-eigen-modem.htm> en <https://www.xs4all.nl/service/diensten/internet/installeren/modem-instellen/hoe-kan-ik-een-ander-modem-dan-fritzbox-instellen.htm>

⁶ https://tele2.gebruikers.eu/forum/view-thread.php?thread_id=3091&pid=27323#post_27323

⁷ <https://forum.t-mobile.nl/t-mobile-thuis-internet-492/gebruik-eigen-modem-t-mobile-thuis-vdsl-276070>

⁸ Zoals glasvezel aanbieder 'Tweak', <https://blog.tweak.nl/hardware/vlan-configuratie-bij-gebruik-eigen-apparatuur/>

Wat dit vooral laat zien is dat het beleid in de praktijk weinig navolging vindt. De consument ontvangt geen of weinig ondersteuning van de aanbieder.

Netwerkinstellingen met eigen modem

Als je geen gebruik maakt van een modem van Telfort, maar liever je eigen modem gebruikt, dan kun je hieronder de netwerkinstellingen vinden.

Netwerkinstellingen zijn de instellingen die je in je modem moet zetten om te kunnen internetten via Telfort Internet. In het modem dat je van Telfort krijgt, zijn deze instellingen al aanwezig. Als je een eigen modem hebt, zal je deze zelf in moeten stellen.

Hieronder staan de algemene instellingen. Het kan zijn dat deze er in je modem anders uitzien. Als je er niet uitkomt, kan je contact opnemen met de fabrikant van je modem en hen deze instellingen geven. Zij kunnen je dan helpen met het instellen van je modem voor het Telfort netwerk.

DSL instellingen (ADSL en VDSL):

- Mode: Routing
- Protocol: IP over Ethernet (IPoE)
- IPv6/IPv4 DualStack: Disable
- Ethernet VLAN Priority/ VLAN ID: 1/34
- IPTV_Ethernet VLAN Priority/ VLAN ID: 5/4
- ADSL VPI/VCI: 0/34
- IPTV_ADSL VPI/VCI: 8/71
- Encapsulation Mode: LLC/SNAP-Bridging
- Service Category: UBR Without PCR
- VDSL VLAN Priority/ VLAN ID: 1/34
- IPTV_VDSL VLAN Priority/ VLAN ID: 5/4
- IP-adres: Dynamic
- Duplex Mode: Auto
- Max Bit Rate: Auto
- DHCP option 60: Enable

Glasvezel instellingen:

- WAN Protocol: MAC Encapsulated Routing
- WAN1 1p/VLAN ID: 1/34
- WAN3 1p/VLAN ID: 5/4
- PPPoE passthrough function: Enable
- IP-adres: 192.168.2.254
- Duplex Mode: Auto
- Max Bit Rate: Auto
- DHCP Server, pool Start IP: 192.168.2.1
- DHCP Server, pool End IP: 192.168.2.252

Tabel 1: Een overzicht van de instellingen zoals deze door Telfort⁹ worden gegeven.

2.5 Ontwikkelingen in Europa ten aanzien van veiligheid & IoT

Er is binnen de Europese Unie sprake van een aantal ontwikkelingen ten aanzien van de veiligheid van gegevens welke gegenereerd worden door het Internet of Things, ook wel bekend als machine-to-machine communicatie. Er wordt op dit moment in de EU gewerkt aan nieuwe regelgeving over de privacy en security van elektronische communicatiediensten en toepassingen die gebruik maken van elektronische communicatiediensten. Het was de vraag tot in hoeverre deze ontwikkelingen rechtstreeks van invloed zijn op de vragen in dit rapport:

De belangrijkste nieuwe regelgeving betreft:

- De European Electronic Communications Code

⁹ Zie: <https://www.telfort.nl/persoonlijk/service/netwerkinstellingen-met-eigen-modem.htm>

- Uitbreiding van de werking van de Radio Equipment Directive en
- De Algemene Verordening Gegevensbescherming (AVG en in het Engels de General Data Protection Regulation GDPR)
- Electronic Privacy Regulation (ePR), welke op dit moment in triloog is tussen de Raad, het Parlement en de Commissie¹⁰
- Cybersecurity Act: Hierin zit een voorstel voor certificatie van cybersecurity Information and Communication Technology cybersecurity certification ("Cybersecurity Act")¹¹

Van de bovenstaande regelingen is de AVG de enige die lopende dit onderzoek in werking is getreden, namelijk op 25 mei 2018. Over de andere regelingen wordt nog onderhandeld, waarbij de ePR in het eindstadium is en de Cybersecurity Act nog aan het begin staat.

Naar verwachting wordt in 2018 de European Electronic Communications Code (EECC) vastgesteld die de huidige EU richtlijnen voor de elektronische communicatiesector vervangt. In de huidige versie van de EECC is een taakstelling opgenomen voor BEREC om lidstaten te adviseren over de interpretatie van het netwerkaansluitpunt. De bepaling heeft als achtergrond dat op dit moment de interpretatie van het netwerkaansluitpunt verschilt tussen lidstaten; ook laat de EECC ruimte in dit opzicht voor een interpretatie die voor verschillende netwerktopologieën anders kan zijn. Een nationale interpretatie van het netwerkaansluitpunt zal echter mogelijk blijven in het kader van het huidige voorstel voor de EECC.

De Radio Equipment Directive (RED) stelt technische eisen aan radioapparaten om op de Europese markt te mogen worden verhandeld. Dit ziet ook op bijvoorbeeld geïntegreerde wifi-modem/routers. Door de IoT-ontwikkeling worden steeds meer apparaten radioapparaten die onder deze richtlijn vallen, zoals een koelkast met een communicatiemodule. De RED biedt tevens de mogelijkheid om (na activering door de Europese Commissie) minimale veiligheids-eisen te stellen aan de digitale veiligheid van bepaalde categorieën van radioapparaten. Dit betreft onder meer de bestendigheid tegen fraude en de bescherming van de privacy in het ontwerp van de apparatuur. Om te voldoen aan deze eisen kan gebruik worden gemaakt van Europees geharmoniseerde standaarden en certificering. Het is de verwachting dat de genoemde eisen op niet al te lange termijn zullen worden geactiveerd voor kwetsbare categorieën radioapparaten. Dit zal met name voorkomen dat nieuwe producten de Europese markt op komen die niet veilig zijn¹².

Bij nadere beschouwing blijkt dat de AVG relatief weinig relevantie heeft voor de vrije modemkeuze. De wetgeving ziet op de verwerking van privacygevoelige gegevens. De rechten en verplichtingen voor betrokken entiteiten veranderen naar ons oordeel niet door een wijziging van de zeggenschap over gebruikte modems in een netwerk.

¹⁰ Het Europees parlement geeft een overzicht van de stand van zaken ten aanzien van de ePR <http://www.europarl.europa.eu/legislative-train/theme-connected-digital-single-market/file-e-privacy-reform>

¹¹ Het Europees parlement geeft een overzicht van de regelgeving rond het cyber security package <http://www.europarl.europa.eu/legislative-train/theme-connected-digital-single-market/file-cyber-security-package>

¹² De meeste huidige door de operator geleverde modems ondersteunen wifi en vallen daarmee onder dergelijke regelgeving. Maar dit betekent ook dat vooralsnog dergelijke eisen niet gelden voor eindapparatuur zonder wifi of andere wireless communicatie-optie.

De genoemde wijzigingen/uitbreidingen van de Europese regelgeving bevatten mogelijk bepalingen op grond waarvan het verplicht is dat apparatuur van beveiligingsupdates voorzien wordt; ook de RED omvat mogelijk deze verplichting (via de genoemde uitbreiding van de werking van deze richtlijn. Of dit de uitkomst wordt van het proces is nu echter nog onduidelijk. Wel is het duidelijk dat op de RED na, de genoemde richtlijnen/verordeningen vooral zien op het verwerken van gegevens door dienstverleners, maar geen beperkingen stelt ten aanzien van de te gebruiken eindapparatuur door gebruikers. De Cybersecurity Act is nu nog in een vroege versie, maar ziet vooral op certificatie van apparatuur naar de mate waarin zij voldoet aan cybersecurity normen. Ongetwijfeld zullen modems en andere eindapparatuur hier onder vallen, maar het is nog onduidelijk of dit de keuze van eindgebruikers kan beperken, doordat bijvoorbeeld netwerkaanbieders eisen kunnen stellen aan het type certificaten waar een apparaat aan moet voldoen voordat het aangesloten kan worden. De mogelijke eisen op het vlak van veiligheid en privacy aan radioapparaten in het kader van de RED werken aanvullend op bijvoorbeeld de Cyber Security Act, die niet over apparaten gaat maar over diensten.

Concluderend kan gesteld worden dat op korte termijn geen wijzigingen worden verwacht in de Europese regelgeving die de implementatie door de EU lidstaten van vrije modem keuze in de relatie tussen telecomaandbieder en telecom-eindgebruiker beïnvloeden. Verwacht kan worden dat de voorgestelde wijzigingen in regelgeving zullen leiden tot een verbetering van de beveiliging van eindapparatuur (waaronder modems) en een betere beveiliging van persoonsgegevens. Het lijkt er echter niet op dat, om dit doel te bereiken, de keuze van consumenten voor eindapparatuur (waaronder modems) beperkt zal worden.

3 Technische achtergrond

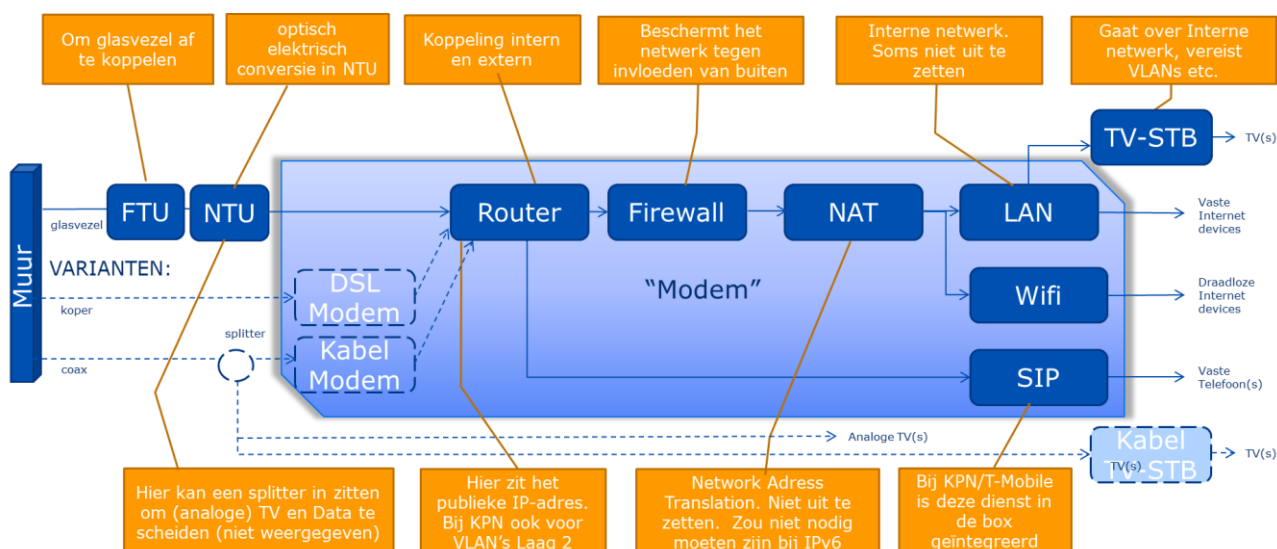
3.1 Analytisch framework voor de analyse van het netwerk

Om de in de consultatie gebruikte argumenten beter te plaatsen is er een technisch analytisch framework nodig: een algemene indeling van netwerken en hun componenten kan de analyse vergemakkelijken en algemene lijnen helderder maken. Voor deze problematiek is het zelfs zo dat twee elkaar aanvullende perspectieven belangrijk zijn: zowel een 'horizontale' als een 'verticale' netwerkindeling is relevant.

Met een horizontale netwerkanalyse wordt het netwerk topologisch ingedeeld. Dat wil zeggen, langs de lijn van netwerkapparatuur vanuit het centrum van het netwerk naar de gebruikers-apparaat toe. De verticale analyse is opgebouwd langs de functionele lagen van een telecom-netwerk, dus vanuit de fysieke verbinding (de kabel zelf), naar de uiteindelijke applicatie (web-sites openen, of smart home applicaties bijvoorbeeld).

3.2 Horizontale netwerk analyse: indeling naar netwerktopologie

Het horizontale netwerk is het meest zichtbaar. Het volgt de apparaten en functies zoals zij vanaf de muur van de woning het huis in komen. Steeds meer functies worden geïntegreerd in hetzelfde apparaat, zoals de Experia-box van KPN en de Connectbox van VodafoneZiggo. Veelal zijn alle functies van modem tot en met Wifi in een apparaat (vaak het modem genoemd) geïntegreerd. VodafoneZiggo kent zelfs de mogelijkheid dat de Mediabox XL, welke normaliter TV-STB is, als modem gebruikt wordt.



Figuur 1: Voorbeeld horizontale indeling netwerkaansluiting (glasvezel)

FTU en NTU

Van buiten komt een kabel (glasvezel, koper of coax) de woning binnen. In het geval van een glasvezelnetwerk gaat deze glasvezel veelal eerst naar een Fibre Termination Unit (FTU). De FTU is een kastje dat als doel heeft om de binnenkomende glasvezel op gecontroleerde wijze (met beperkte kans op beschadiging) te koppelen op het modem of een interne glasvezel. De FTU is een passief element en bevat geen elektronica. In enkele gevallen, zoals bij bepaalde 'Reggefiber woningen' wordt het optische signaal vertaald naar een elektrisch signaal door een signaalomzetter ook wel bekend als Network Termination Unit (NTU) en daarna doorgeleid naar het kastje dat meestal wordt aangeduid met 'de modem'. Strikt genomen zou de glasvezel NTU gezien kunnen worden als een modem omdat hier optisch elektrische conversie van het signaal gebeurt, maar hier gebeurt verder inhoudelijk niets met het signaal.

In bovenstaande figuur is de situatie in glasvezelnetwerken als uitgangspunt genomen maar zijn enkele varianten in stippellijnen getekend. In kabelnetwerken, enkele FTTH-netwerken en ISDN in combinatie met Internet wordt gewerkt met een splitter, zodat bijvoorbeeld een signaal van de Centrale Antenne Televisie (CATV) afgesplitst kan worden. Dit biedt eindgebruikers de mogelijkheid om een digitaal/analoog kabel-signaal voor radio en TV over de bestaande coaxkabel in huis te leiden.¹³

De modem en de router

Na de FTU en eventuele signaalconversie en/of splitter wordt een modem aangesloten. Een modem moduleert en demoduleert signalen op een medium (bijvoorbeeld een koper draad of radiosignaal). In moderne internetnetwerken ontvangt een modem de IP-pakketten van het interne netwerk en zet deze om naar een codering en een signaaldrager voor het externe netwerk en vice versa. Het doet soms ook nog een vorm van authenticatie (bv PPPoE). Het verschil tussen een modem en een signaalconverteer is dat een modem indien nodig ook een omzetting doet van de gebruikte protocollen, bijvoorbeeld van het intern gebruikte Ethernet naar VDSL, Docsis, GPON of de extern gebruikte variant van Ethernet. Modem, router, firewall, NAT, switch en Wifi zijn veelal geïntegreerd in hetzelfde kastje dat klanten van hun ISP krijgen. Telefonie (SIP) is veelal ook geïntegreerd, terwijl voor televisie meestal een aparte set-top box gebruikt wordt.

De router verbindt interne en externe netwerken met elkaar op het niveau van het internet protocol. De router weet waar de IP-adressen zich bevinden, in het interne netwerk of in het externe netwerk. In het geval van bedrijfsaansluitingen kan de router er ook voor zorgen dat het verkeer voor redundantie over twee aansluitingen geleid wordt, bijvoorbeeld zowel een kabel als een DSL aansluiting.

Verskil in firewalls

De firewall filtert het verkeer en blokkeert datgene wat niet toegestaan is. Een firewall kan zich zowel voor als na de router bevinden. De firewalls die actief zijn in apparaten die door

¹³ Er zijn verschillende FTU's en NTU's in omloop en er zijn verschillende webpagina's en de Youtube-filmpjes welke de verschillende oplossingen uitleggen, voor bijvoorbeeld zelfinstallatie. Zie bijvoorbeeld Fiber.nl's Youtube kanaal waar verschillende instructiefilmpjes voor zelf-installatie te vinden zijn. Een handleiding voor een FTU, met geïntegreerde CATV splitter, modem, router en telefonie bevindt zich op <https://www.fieber.nl/wp-content/uploads/2015/12/Genexis-FXP-KIT-125-Genexis-Ombouwset-GN01-GN02.pdf>

ISP's geleverd worden zijn veelal vrij gebruiksonvriendelijk van aard. Consumenten elektronica fabrikanten leveren ook firewalls in hun apparatuur die meer gebruikersvriendelijk zijn. Het verschil tussen de twee is dat de firewalls van de ISPs bijvoorbeeld vereisen dat iedere website die geblokkeerd moet worden handmatig toegevoegd moet worden. De gebruikersvriendelijke firewalls geven de mogelijkheid om per apparaat in huis aan te geven wanneer deze toegang tot het internet mag hebben, ze filteren op basis van automatisch gevulde lijsten met schadelijke of illegale content en ze scheiden gasten van thuisgebruikers.

Externe en interne IP adressen

Network Address Translation (NAT) is nodig omdat er te weinig publieke internet adressen zijn voor alle apparaten die tegenwoordig aan het internet gekoppeld zijn. Om die reden wordt in een thuisnetwerk veelal gebruik gemaakt van 1 extern IP-adres en een intern netwerk op basis van IP-adressen uit (bijvoorbeeld) de reeks 192.168.x.x. Iedere keer als er een verbinding naar buiten gemaakt wordt, krijgt die verbinding een eigen poortnummer toegewezen, zodat het verkeer dat op die poort terug komt naar het juiste apparaat in huis geleid kan worden. In veel apparaten die door ISPs geleverd worden kan de NAT-functie niet uitgezet worden, hetgeen kan leiden tot conflicten met andere apparaten, bijvoorbeeld een mesh-wifi systeem dat door de gebruiker zelf is aangeschaft. Dergelijke systemen hebben ook hun eigen NAT-functie aan boord en dit zorgt voor een dubbele NAT, hetgeen voor problemen kan zorgen, doordat het poortnummer aan de buitenkant bij de vertaling naar de binnenkant verloren gaat.¹⁴

Wat doet een switch?

De switch is het deel van het apparaat dat het interne netwerk verkeer in het huis regelt. Het ontvangt verkeer van apparaten welke middels Wifi of via kabels aangesloten zijn. De meeste apparaten van ISPs hebben 4 poorten beschikbaar voor het interne netwerk. Het aantal apparaten is in veel huizen veel groter, zodat veel gebruikers meerdere losse switches in huis hebben staan (soms geïntegreerd met een wifi-access point). Deze functioneren als het netwerk equivalent van een stekkerdoos; het mogelijk maken dat op 1 netwerkpoort meerdere apparaten aangesloten kunnen worden. Providers als KPN en VodafoneZiggo leveren dit soort switches ook aan hun klanten, veelal om de Wifi in huis uit te breiden. De switch is veelal geïntegreerd met het Wifi netwerk. In toenemende mate worden ook interne Internet of Things (IoT) netwerken, zoals bijvoorbeeld een Zigbee gateway voor de Philips Hue lampen gekoppeld op een poort op een switch.

Een geïntegreerd apparaat

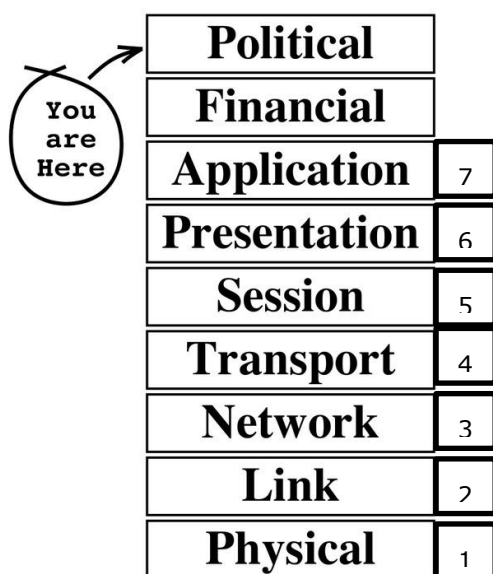
Veel ISPs leveren een apparaat dat ook Wifi ondersteunt en als access point functioneert. In recente jaren is de werking van het Wifi belangrijker geworden voor ISPs om zich te profileren. De positie van het modem in de meterkast is veelal niet goed genoeg om dekking in het hele huis te realiseren. Gebruikers gingen zelf op zoek naar oplossingen en zetten bijvoorbeeld op de etages een los access point neer. Dit vergt een kabel naar boven, enige configuratie van de gebruiker en zorgt nog niet voor een naadloze overgang. VodafoneZiggo en KPN leveren nu ook geconfigureerde access points, die functioneren als combinatie van switch en access point, maar nog niet een naadloze overgang bieden. De markt is alweer verder. Fabrikanten als

¹⁴ Dit is een bekend fenomeen voor spelers van online games die uitgenodigd worden door andere spelers, waar de gamecomputer niet bereikbaar is voor uitnodigingen door de dubbele NAT.

Google, Linksys, TP-Link en anderen bieden Wifi-mesh systemen die niet alleen naadloze verbinding beloven, maar ook geen kabel nodig hebben en bovendien geavanceerdere vormen van firewall, ouderlijk toezicht, toegangscontrole en gasten-wifi bieden. Deze access points komen echter met een geïntegreerde Router, firewall, NAT en switch en leiden tot situaties met dubbele NAT.

3.3 Verticale netwerkanalyse: het functionele lagenmodel

Een andere manier van kijken naar netwerken is door een netwerk te zien als een combinatie van lagen. Plastisch gezegd, een netwerk is een samenstel van kabels of draadloze verbindingen, op die verbindingen wordt een elektromagnetisch of lichtsignaal gezet, in deze signalen zitten signalen om de verbinding mogelijk te maken, om routing mogelijk te maken en de eigenlijke inhoud welke gecommuniceerd moet worden. Deze wijze van analyseren is ooit gestandaardiseerd in een het OSI-lagenmodel¹⁵, welke uiteindelijk opgevolgd is door een meer praktische interpretatie van het IP-lagenmodel, waarbij sessie en presentatie geen rol spelen.



Figuur 2: Voorbeeld verticale indeling: functionele lagen geïnspireerd door OSI model, met rechts de veelgebruikte nummering van de OSI lagen. De twee bovenste lagen werden ooit als grapje toegevoegd door Evi Nemeth, maar hebben een sterke kern van waarheid¹⁶

Historisch gezien heeft het OSI-lagenmodel 7 lagen welke van onderaf geteld worden, waarbij de fysieke laag, laag 1 is en de applicatie laag, laag 7 is. Nog steeds gebruiken netwerksspecialisten deze nummers.

¹⁵ Het **OSI-model** is een door [ISO](https://nl.wikipedia.org/wiki/ISO) gestandaardiseerd referentiemodel voor datacommunicatiestandaarden, ter bevordering van de interoperabiliteit tussen heterogene [netwerktopologieën](https://nl.wikipedia.org/wiki/netwerktopologie). Het [acronym](https://nl.wikipedia.org/wiki/acronym) **OSI** staat voor: **O**pen **S**ystems **I**nterconnection <https://nl.wikipedia.org/wiki/OSI-model>

¹⁶ gebaseerd op de interpretatie van het OSI model door Evi Nemeth, zie <https://www.linuxjournal.com/article/10726>

De belangrijkste laag is laag 3. Dit is de netwerk laag en de laag waar het Internet Protocol (IP) zich bevindt. Het Internet Protocol maakt het mogelijk om verschillende fysieke netwerken met elkaar te verbinden en de applicaties die hier overheen gingen met elkaar te laten communiceren. Dit alles ook nog eens zonder dat beide netwerken elkaars topologie (fysieke en logische netwerkstructuur) hoeven te kennen. Er is wel een vergelijking gemaakt met containers in de logistiek, waar containers op alle onderliggende netwerken (rails, weg en water) functioneren en alle mogelijke vormen van inhoud (bulk, voedsel, kleding, machines) meedragen.

Een bekende grap met een serieuze ondertoon is de toevoeging van laag 8 en 9 als zijnde financieel en politiek. Deze twee lagen spelen ook hun rol bij de keuze van waarom een netwerk of dienst op een bepaalde manier in elkaar gezet is. In dit rapport betreft laag 8 de operationele keuzes van de ISP, welke geanalyseerd zijn in dit rapport. Laag 9 is voor dit onderzoek de tekst van de regelgeving.

Van een netwerk per toepassing naar een netwerk voor alle toepassingen

Voordat het Internet Protocol gemeengoed was, was het mogelijk om twee verschillende bedrijfsnetwerken met elkaar te verbinden, maar dit vergde veel moeite en werd erg duur.

IP veranderde dit. Het behandelde verzonden verkeer als een serie pakketjes in pakketjes (zoals een Russische Matrushka pop). Het enige dat het onderliggende netwerk nu moest doen is zo snel mogelijk de pakketjes van a naar b te sturen. Door deze lagen hoeven de applicaties niet te weten hoe het onderliggende netwerk werkt. De onderliggende netwerken hoeven niet te weten wat voor soort inhoud ze versturen. IP werkt als laag die de twee verbindt. Zolang applicaties maar weten naar welk IP-adres ze sturen en netwerken maar weten in welke richting (niet de exacte locatie) het adres zich bevindt werkt alles heel simpel en eenvoudig.

De uitvinding van IP had twee gevolgen:

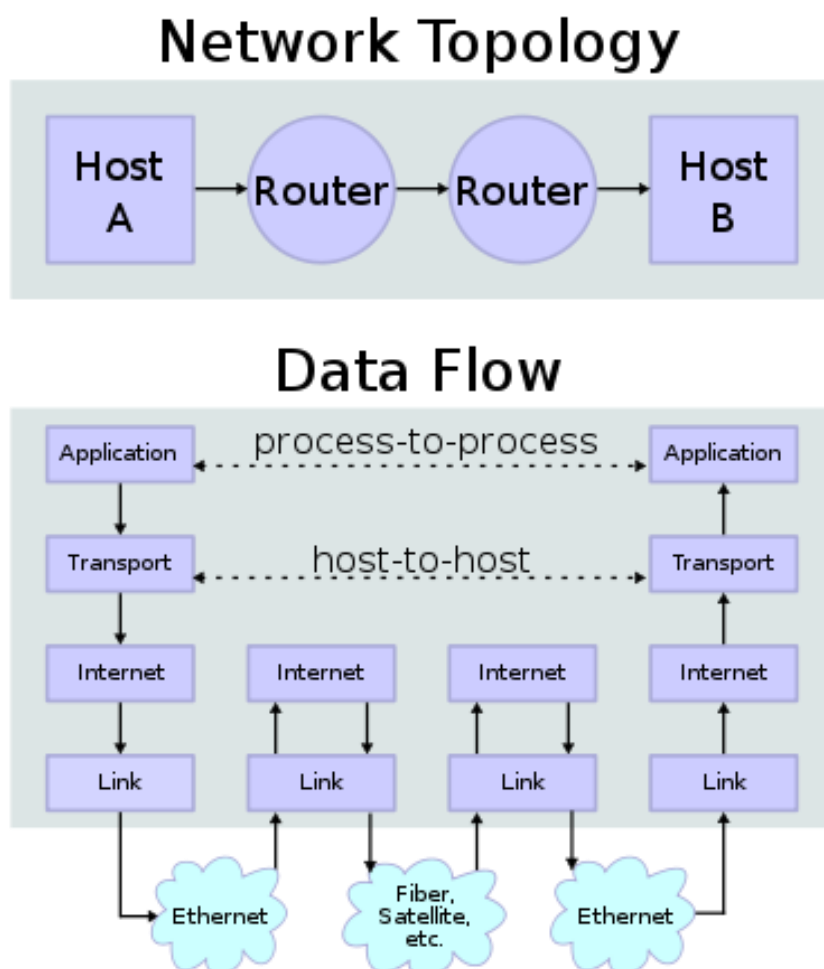
1. Het werd mogelijk om zeer uiteenlopende netwerken met elkaar te verbinden. Juist daarom werd het zeer populair in academische kringen. Academische netwerken waren een mengelmoes van experimentele netwerk protocollen en architecturen, nationale telecomnetwerken en verschillende generaties van oude netwerken welke nooit vervangen waren, maar wel van groot belang waren. Als beide partijen IP spraken, dan werd het een stuk eenvoudiger om bijvoorbeeld supercomputers, deeltjesversnellers of telescopen met elkaar te verbinden, want dan was er minder omzetting nodig.
2. De macht van de fabrikanten van netwerken nam dramatisch af. Voor de uitvinding van IP was het veelal goedkoper en eenvoudiger om de volgende generatie van hetzelfde netwerkprotocol te gebruiken, omdat deze veelal met elkaar konden samenwerken. Na de uitvinding van IP kon een oud netwerk eenvoudig aan een nieuw netwerk gekoppeld worden. Keuzes uit het verleden bepaalden niet meer de toekomst. Ook veel nationale versies van protocollen, gepromoot door nationale telecomorganisaties of fabrikanten werden minder acceptabel omdat ze veelal IP niet ondersteunden.

Het adagium werd dan ook: "Alles over IP en IP over alles". Waar voorheen televisie, telefonie, mobiele communicatie, e-mail en andere systemen allemaal hun eigen netwerk en protocollen hadden werd het een race om alles over IP te krijgen. Er was wel een trade-off; een eigen netwerk voor één specifieke dienst, bijvoorbeeld mobiele telefonie of televisie, kan helemaal

geoptimaliseerd worden voor die ene dienst. Dit is voor die dienst misschien efficiënter, maar is niet optimaal in een dynamische wereld met meerdere diensten. Het kan zijn dat televisie en telefonie beter over een eigen speciaal ontwikkeld netwerk passen, maar een flexibel, general purpose netwerk is uiteindelijk handiger voor veel verschillende toepassingen. En net als in de containerindustrie heeft de markt zich aangepast door een veelheid van toepassingen welke vroeger over een eigen netwerk gingen nu in een aangepast formaat over IP te zenden. Door IP is het mogelijk de toepassing wereldwijd uit te rollen. Dit is ook de reden waarom modems van nu ook invloed kunnen hebben op de applicaties die in het thuisnetwerk gebruikt worden zoals televisie en telefonie, terwijl het gevoel vooral heerst dat modems alleen over de verbinding met het internet gaan.

3.4 Bruikbaarheid modellen bij validatie

In de analyse en validatie van argumenten uit de consultatie in dit rapport spelen alle lagen maar ook vele onderdelen uit de topologie een rol omdat beide modellen bij end-to-end communicatie van belang zijn. Dit wordt geïllustreerd door Figuur 3.



Figuur 3: Combinatie van horizontale en verticale modellering voor illustratie van end-to-end communicatie¹⁷.

Bij de analyse wordt waar nodig per argument aangegeven welke lagen er bij betrokken zijn en welke deel van het netwerk het betreft. Op deze wijze kunnen de argumenten op een uniforme wijze geanalyseerd worden.

¹⁷ Bron: wikipedia, https://nl.wikipedia.org/wiki/Protocol_stack

4 Inventarisatie en groepering issues

In dit hoofdstuk bespreken we de reacties op de consultatie “vrije modemkeuze”. We beschrijven het aantal reacties, de aard van de argumenten en welke soorten partijen achter de openbare reacties zitten. Ook schetsen wij welke zaken ons het meest opvielen in de reacties.

4.1 Overzicht en achtergrond reacties

Er zijn in totaal 63 consultatiereacties binnengekomen, waarvan 1 een duplicaat en 1 leeg. Van de 63 reacties zijn 34 geclassificeerd als openbaar en 29 als niet-openbaar. 9 reacties waren voorzien van een toelichting in een bijlage. In Annex B kunt u een samenvattende tabel vinden waar de hoofdlijnen van alle openbare reacties te zien zijn. Annex C bevat een tabel met de niet-openbare reacties.

Er waren twee reacties namens een groep bedrijven: één gezamenlijke reactie door Bird&Bird namens CAIW, KPN, de aanbieders verenigd in NLConnect, Tele2, T-Mobile, en VodafoneZiggo, en één reactie van een vereniging van Europese fabrikanten van eindapparatuur (Verbund der Telekommunikations-Endgerätehersteller "VTKE"),

NLConnect is een vereniging van een aantal voornamelijk middelgrote en kleine Nederlandse kabel- en telecombedrijven¹⁸: CAIHarderwijk, CAIW, Cambrium, Delta, e-Fiber, CAI Edam-Volendam, Geuzenet, Glasnet, InCompanyMedia, Jonaz (Rotterdam), Kabelnoord, Kabeltex, KT Waalre, Matrix ICT, OpenFiber, PhotonicNetworks, Plinq, SKP(Pijnacker), SKV (Veendam), Teleplaza, Trined (Eindhoven), Webservice, Youfone.

Daarnaast waren er 4 reacties van afzonderlijke telecombedrijven en 8 van andere bedrijven zoals kleinere ICT bedrijven en ZZP'ers. De overige 49 reacties zijn van particulieren.

In de volgende paragrafen wordt een samenvatting gegeven van de belangrijkste issues die in de consultatie naar voren komen, en worden de issues ingedeeld in een aantal categorieën. Deze indeling is niet gedaan vanuit één gezichtspunt. We zien in Tabel 2 dat, afhankelijk van het gezichtspunt, hier verschillende indelingen mogelijk zijn. Elke indeling volgens één gezichtspunt heeft zijn beperkingen, omdat onderwerpen die niet samenhangen met het gezichtspunt dan bij verschillende onderdelen van de indeling herhaald worden. Het gebruik van verschillende indelingen betekent echter ook herhaling van onderwerpen.

¹⁸ Inmiddels zijn op 19 april 2018 ook de FiberSociety (voorheen FttH platform en e-Society platform, verenigde uiteenlopende partijen in hun streven naar glasvezel) en de Vefica (verenigde fabrikanten en leveranciers breedbandindustrie) toegetreden tot NLConnect

Topologie:	Service Aspecten:	Achterliggende doelen:	Stakeholders:
- Impact op <i>apparatuur</i> (andere apparatuur dan het modem) - Impact op <i>diensten</i> (internettoegang, TV, telefonie, ...) - Impact op <i>openbare netwerken</i> - Impact op <i>private netwerken</i> (thuisnetwerk)	- <i>Authentication, authorisation, accounting</i> - <i>Network management</i>, onderhoud en upgrades - <i>Storingsdetectie en storingsafhandeling</i>	- Duidelijke verantwoordelijkheden - <i>Veiligheid (safety & security)</i> - <i>Innovatie</i> - <i>Ontzorging</i> - <i>Keuzevrijheid</i> - <i>Concurrentie</i> - <i>Interoperabiliteit en standaardisatie</i> - <i>Privacy</i>	- <i>Eindgebruiker</i>: van netwerktoegang of van diensten - <i>Fabrikanten</i>: apparatuur aanbieders: modems, access points, routers, ... - <i>Toegangsaanbieder</i>: glasvezeltoegang, kabeltoegang, DSL toegang, maar denk ook aan: combinatie vast/mobiel (buitengebied) - <i>Dienstenaanbieder</i>: internettoegang, Televisie, Telefonie, ...

Tabel 2: Verschillende indelingen zijn denkbaar om reacties te categoriseren, elk met hun eigen gezichtspunt, en elk eigen voor- en nadelen.

Deze "indelingsparadox" is nooit helemaal op te lossen. In dit onderzoek is daarom een pragmatische indeling gebruikt die een mix is van verschillende gezichtspunten¹⁹:

De gebruikte indeling is:

- **Netwerkbeheer**: issues uit de consultatiereacties die betrekking hebben op de optimalisatie, continuïteit en kwaliteit van toegang tot het operator netwerk, deze worden beschreven in paragraaf 4.2.
- **Veiligheid**: issues uit de consultatiereacties die betrekking hebben op het waarborgen van de veiligheid van operator netwerken en de integriteit van de daarover uitgewisselde informatie. Dit betreft zowel risico's vanuit het openbare netwerk op private netwerken als vice versa. Deze issues worden beschreven in paragraaf 4.3.
- **Diensten**: issues uit de consultatiereacties die verband houden met de implicaties voor diensten die door eindgebruikers worden afgenomen. Deze issues worden beschreven in paragraaf 4.4.
- **Eigen netwerk en apparatuur**: dit betreft issues uit consultatiereacties die verband houden met de flexibiliteit en veiligheid van het eigen netwerk van consumenten en bedrijven. Deze issues worden beschreven in paragraaf 4.5
- **Regelgeving**: issues met betrekking tot definities van regelgeving, consistentie, samenhang met andere regelgeving, timing, planning, handhaving, etc. Deze issues worden beschreven in paragraaf 4.6.
- **Standaarden netwerkaansluiting**: issues uit de consultatiereacties die ingaan op (technische) standaardisatie als mogelijke oplossingsrichting. Ook bevat deze

¹⁹ Deze indeling is zodanig gekozen dat de issues niet in te veel verschillende categorieën terecht komen en dat de issues enigszins logisch zijn verdeeld. Het blijft echter een subjectieve categorisering, waarbij overlap onvermijdelijk is.

categorie issues die betrekking hebben op hoe de klant aangesloten is in de meterkast, vooral met betrekking tot FTTH, dat door de operators als kwetsbaar wordt gezien. Deze zijn beschreven in paragraaf 4.7.

- **Overige opvallende reacties:** een bloemlezing van opvallende reacties die niet in één van de bovenstaande categorieën passen, is te vinden in paragraaf 4.8.

De volgende paragrafen in dit hoofdstuk vatten de belangrijkste issues samen. In de Annex A is een uitgebreidere samenvatting te vinden waarbij per issue verwezen wordt naar relevante consultatiereacties waarin dit issue besproken wordt, via een code (van de vorm "[ABC]") die verwijst naar de codes in Annex B en Annex C.

4.2 Netwerkbeheer

Hieronder vallen onder andere de in de consultatiereacties genoemde issues rond verkeersmanagement, impact op architectuur, impact tussen verbindingen onderling (onder andere voor DOCSIS en VDSL) en de omvang hiervan (o.a. kwaliteit vs. verstoring netwerktoegang). De belangrijkste in de consultatie genoemde issues die impact hebben op netwerktoegang tot het operator netwerk zijn:

- Instellen eigen modem of gebruik oud modem leidt mogelijk tot slechtere prestaties of storingen.
- Bij Docsis 3.x en VDSL is de kwaliteit van de doorgifte van het signaal voor een gehele wijk afhankelijk van het functioneren van alle modems in die wijk.
- Prestatiegaranties zijn aan klanten met eigen modem niet of in mindere mate te geven.
- Bepaalde varianten van wholesale aanbod zijn moeilijker te realiseren
- Service Level Agreements (SLA's) zijn moeilijker te handhaven omdat monitoring en rapportage moeilijker wordt.
- Het is onduidelijk of apparatuur die via thuis- of bedrijfsnetwerken wordt gebruikt voor mobiele netwerken binnen of buiten de beleidsregel valt.
- Er is mogelijk een grotere kans op fysieke schade als het demarcatiepunt niet na een modem of aansluitapparaat ligt.
- Sommige hybride oplossingen worden moeilijker te realiseren.

De genoemde issues worden in Annex A in paragraaf 0 kort beschreven.

4.3 Veiligheid

Deze categorie bevat issues rond het waarborgen van de veiligheid van operator netwerken en de integriteit van de daarover uitgewisselde informatie. Hieronder vallen onder andere: authenticatie, autorisatie en encryptie en bijbehorende operationele risico's (onder andere gemak uitwisseling encryptiesleutels). Het gaat hier ook om de risico's vanuit private netwerken op openbare netwerken, zoals de gevolgen van DDOS aanvallen en botnets voor het openbare netwerk.

De belangrijkste in de consultatie genoemde issues die impact hebben op veiligheid zijn:

- Algemene zorgen van operators over de gevolgen van de beleidsregel voor de netwerkveiligheid.

- Klant zelf modem laten instellen kan netwerkveiligheid verlagen.
- Er zijn ook argumenten dat veiligheid juist gediend is bij diversiteit in modems en instellingen. Veiligheid is mogelijk niet 1 op 1 gerelateerd aan de toegangsfunctie.
- Beschikbaarheid goedkope onveilige apparaten versterken veiligheidsrisico's van en voor private netwerken.
- Hardware leveranciers geen belang bij pushen updates (eenmalige levering), bouwen geen daarvoor noodzakelijke klantrelatie op, klanten doen zelf geen handmatige update.
- De uitzonderingen in artikel 1.5 ten aanzien van een bij het netwerk behorende identificatie- authenticatie- of beveiligingsfunctie leveren discussie op bij zowel voor- als tegenstanders van de beleidsregel.

De genoemde issues worden in Annex A in paragraaf A.2 kort beschreven.

4.4 Diensten

Deze categorie betreft reacties rond de implicaties voor en door diensten die door eindgebruikers worden afgenomen en zaken als Digital Rights Management (DRM)

De belangrijkste in de consultatie genoemde issues die impact hebben op diensten zijn:

- Issues rond TV set top boxen en DRM management: vallen ze wel of niet onder de beleidsregel? Doorgeven van auteursrechtelijk beschermde content noodzaakt soms gebruik van bepaalde voorgeschreven hardware.
- Issues rond diensten als telefonie en (publieke) Wifi Hotspots aangeboden op of gefaciliteerd door eindapparaten. Ook hier is de reikwijdte van de regeling soms onduidelijk. Apparatuur die noodzakelijk is voor bepaalde diensten zou volgens sommige reacties deel moeten uitmaken van het operator netwerk. Volgens andere reacties juist niet.

De genoemde issues worden in Annex A in paragraaf A.3 kort beschreven.

4.5 Eigen netwerk en apparatuur

Dit betreft zaken als veiligheid en flexibiliteit van het eigen netwerk van consumenten en bedrijven en de daar aangesloten apparatuur. Hieronder vallen onder andere: het ontbreken van een firewall voor inkomend en/of uitgaand verkeer en de omvang hiervan (onder andere hoe groot is het probleem relatief als allerlei andere apparaten ook kwetsbaar zijn), DDoS aanvallen vanuit andere apparaten op het thuisnetwerk (onder andere de voor- en nadelen van centraal management firewalls etc.);

De belangrijkste in de consultatie genoemde issues die impact hebben op eigen netwerken van consumenten en bedrijven en de daarop aangesloten apparatuur zijn:

- Verschillende percepties over hoe flexibel de huidige situatie is ten aanzien van de flexibiliteit van de thuis- en bedrijfsnetwerken.
- Een roep om de verantwoordelijkheden voor apparatuur beter te scheiden.

De genoemde issues worden in Annex A in paragraaf A.4 kort beschreven.

4.6 Definities en consistentie van regelgeving

Hieronder vallen reacties die ingaan op definities van regelgeving en consistentie daarvan en samenhang met andere regelgeving, en issue rond procedure, planning en handhaving van de regelgeving.

De belangrijkste in de consultatie genoemde issues die impact hebben op regelgevingstechnische issues zijn:

- Huidige regelgeving biedt mogelijkheden, maar deze wordt niet voldoende gehandhaafd.
- Het achterliggende probleem dat deze regelgeving wil oplossen is onduidelijk.
- De beleidsregel is geen verduidelijking maar een wijziging van bestaande regelgeving en dat kan niet zondermeer via een beleidsregel.
- De timing van de procedure is onduidelijk.
- Er is mogelijk strijdigheid met andere regelgeving.
- De formulering is niet eenduidig.

De genoemde issues worden in Annex A in paragraaf 0 kort beschreven. Deze issues worden in dit document in de analyse verder niet behandeld, omdat dit onderzoek een technische second opinion betreft en de regelgeving out of scope is.

4.7 Standaarden netwerkaansluiting

Deze categorie bevat issues en argumenten uit de consultatiereacties die ingaan op standaarden of standaardisatie als mogelijke oplossingsrichting, specificaties, of issues rond de standaardisatie van de passieve netwerkaansluiting in de meterkast

De belangrijkste in de consultatie genoemde issues die impact hebben op apparatuur- en aansluitstandaarden zijn:

- Er zijn aansluitstandaarden nodig voor interoperabiliteit en flexibiliteit.
- De standaarden die er zijn, zijn niet interoperabel en uniform.
- Er is een informatieplicht nodig om het omgaan met veranderende standaarden te faciliteren.
- Techniek ontwikkelt zich snel, publicatie specificaties vertraagt innovatie.
- Techniek wordt gefaseerd over regio's uitgerold. Netwerkspec alleen in nieuwste versie te publiceren, per regio/adres is onwerkbaar.
- Er moet voorkomen worden dat een interfacebeschrijving of standaard de keuzevrijheid juist beperkt.

De aanbieders brengen naar voren dat de wijze waarop de Beleidsregel omgaat met de passieve aansluiting in de meterkast niet strookt met de bestaande praktijk. Zij noemen een aantal issues, met name ten aanzien van glasvezelaansluitingen:

- *Er mag geen NT (NTU) meer aangelegd worden.*
- *Zonder NT geen overeengekomen kwaliteit.*
- *Aansluiten kan alleen door vakbekwame monteurs.*

De genoemde issues worden in Annex A in paragraaf A.6 kort beschreven. In de analyse zal dit punt met name worden meegenomen in de paragraaf over het passieve aansluitpunt.

4.8 Overige opvallende reacties

De reacties laten een divers beeld zien waarbij zowel tevredenheid als ontevredenheid met de huidige situatie elkaar afwisselen waarbij de paradox tussen wensen ten aanzien van flexibiliteit, veiligheid en ontzorging opvalt. Ook krijgt de gedachte achter de beleidsregel zowel support als kritiek. Zo is er de hoop dat er meer vrijheid en flexibiliteit is voor gebruikers met kennis en dat concurrentie wordt gestimuleerd, maar ook de vrees dat het voor de minder ervaren eindgebruiker uiteindelijk ingewikkelder en duurder wordt. Ook is er bezorgdheid dat implementatie van de voorgenomen beleidsregel tijd kost door benodigde herinrichting van processen.

In Annex A bevat paragraaf A.7 een bloemlezing uit overige genoemde issues, meningen, zorgen, observaties etc. Deze issues worden in dit document in de analyse verder niet behandeld, omdat dit onderzoek een technische second opinion betreft en de regelgeving out of scope is.

5 Analyse: Validatie technische argumenten

Aan de hand van de in het vorige hoofdstuk beschreven categorieën wordt in dit hoofdstuk een analyse uitgevoerd van de belangrijkste issues die in de consultatie naar voren kwamen. Hierbij wordt globaal de indeling uit het vorige hoofdstuk gebruikt²⁰,

Per sectie worden eerst de belangrijkste effecten beschreven, vervolgens wordt een analyse en validatie beschreven, met name vanuit technologisch perspectief, en wordt afgesloten met één of meer conclusies.

5.1 Issues rond impact op Operator Network

5.1.1 Belangrijkste effecten

Netwerk operators en ISP's leveren aan klanten een netwerksignaal dat over een kabel of door de ether naar de eindgebruiker gaat. Er is een veelheid van modulatie technieken die gebruikt worden om de communicatie mogelijk te maken. Te denken valt aan verschillende varianten van DSL (koper), Docsis (kabel), Ethernet (FTTH), GPON (FTTH), GSM/UMTS/LTE (mobiel) en fixed/wireless. Er is binnen elk van deze standaarden een veelheid aan technische parameters die ingesteld kunnen worden om een optimale verbinding richting de eindgebruiker te realiseren.

Vanuit de kant van de aanbieders wordt gesteld dat zij controle over het modem deel van de verbinding nodig hebben, "omdat alleen op die manier zij alleen dan de hele keten tussen de locatie van de eindgebruiker en het eigen netwerk te bewaken en te besturen. Slechts dan kan de Aanbieder de eindverantwoordelijkheid dragen voor de prestaties van die keten ten opzichte van de klant en de eisen van de overheid." [BIR].

Netwerkaanbieders noemen als argument onder andere:

- *Modem bepaalt performance:* Bij verschillende typen netwerken (HFC, VDSL) is de kwaliteit van de doorgifte van het signaal voor een gehele wijk afhankelijk van het functioneren van alle modems in die wijk. Een 'vreemd', onbekend modem kan daarbij negatieve impact hebben op kwaliteit van andere aansluitingen.
- *Storingen:* In een hybrid coax-fiber (HFC) netwerk gaat het om gedeelde toegang. De kwaliteit van het signaal is afhankelijk van het functioneren van alle modems in die wijk. Een onbekend modem kan een negatieve impact hebben op de dienstverlening voor alle aangeslotenen in de wijk. Als niet duidelijk is van welk modem het stoorsignaal komt, dan moeten een voor een alle afgaande takken onderzocht worden, bv door loskoppeling.
- *Wholesale aanbiedingen:* Voor open glaswerken geldt dat zij op 2 lagen dienstverlening bieden aan andere ISP's: 1. Er zijn ISPs met eigen actieve apparatuur in de meterkast van de eindgebruiker en 2. ISPs die de NTU van de netwerkbeheerder

²⁰ met uitzondering van de niet technisch georiënteerde categorieën "definities en consistentie regelgeving" (paragraaf 4.6) en "overige opvallende reacties" (paragraaf 4.8).

gebruiken en daar een eigen router achter plaatsen. In dit laatste geval kan de netwerkaanbieder niet de kwaliteit van de verbinding richting zijn wholesale klant monitoren en garanderen.

- *Internetsnelheden:* Een aanbieder moet de minimale, normaliter beschikbare, maximale en de geadviseerde download- en uploadsnelheid van internettoegangs-diensten communiceren. Als een gebruiker een eigen modem gebruikt, dan kan de aanbieder geen adequate informatie verstrekken.
- *Interoperabiliteit:* De praktijk ten aanzien van technische standaarden is weerbarstig. Ook wanneer fabrikanten dezelfde standaarden toepassen, kunnen er interoperabiliteitsissues optreden. Standaardisatie laat onbedoeld nog wel eens ruimte voor verschillende invullingen. Daarbij zijn er ook specifieke functionaliteiten welke aanbieders buiten de standaarden om aanbieden. Aanbieders certificeren om deze reden apparatuur voor hun netwerken.
- *Combineren 4G/DSL:* Bij sommige oplossingen worden access technologieën gecombineerd (bijvoorbeeld DSL/4G. Hiervoor is apparatuur bij de klant nodig. Deze apparatuur is per definitie nog deel van het netwerk.

5.1.2 Validatie van de technische argumenten

Breedbandnetwerken zijn in de laatste jaren veranderd. Zoals ook in hoofdstuk 3 geschetst, worden toegangsnetwerken, zoals het van oorsprong telefonienetwerk PSTN en van oorsprong TV distributienetwerk coaxkabelnetwerk nu ingezet voor doeleinden waarvoor ze initieel niet ontwikkeld zijn. Om steeds meer bits over een vergelijkbaar stuk netwerk heen te krijgen is er een aantal wijzigingen in het netwerk aangebracht:

- Verkorten van de koperverbindingen in het netwerk en het dichterbij brengen van de glasvezelinfrastructuur.
- Het verbreden van het spectrum waarover signalen verstuurd worden.
- Het coördineren en combineren van het signaal van de modems.
- Het verhogen van het aantal bits op een Hertz.
- Het inzetten van overspraak en andere traditioneel als negatief ervaren effecten voor het verhogen van de performance.

Dit heeft tot effect dat de netwerken gevoeliger voor verstoring kunnen worden. Voor ieder van de netwerken zal nu beoordeeld worden wat de vrije modem keuze voor effect kan hebben.

Kopernetwerken

Voor PSTN gebaseerde netwerken heeft dit geleid tot bonded VDSL en g.Fast; op kabelnetwerken brengt dit Docsis 3.0 en 3.1. Dit heeft ertoe geleid dat dergelijke netwerken niet meer beheerd worden als discrete lijnen, maar als een systeem waarbij elke modem afgestemd wordt op een andere modem. Op deze wijze kan er uit het gehele systeem meer performance gehaald worden dan uit de som der delen.

Fabrikant gebonden apparatuur alleen in uitzonderingsgevallen noodzakelijk

In veel gevallen kan hierbij in één netwerk gebruik gemaakt worden van apparatuur van verschillende fabrikanten, zolang er maar aan de standaard c.q. specificaties van het netwerk voldaan wordt.

Door de fabrikanten en telecomnetwerken worden er zogenaamde "plugfests" georganiseerd om te testen of de apparatuur van verschillende fabrikanten de standaarden op vergelijkbare manier interpreteert en functioneert in de praktijk, en dus met elkaar kan samenwerken. Uit communicatie rond deze plugfests blijkt dat alle bekende fabrikanten mee doen aan dergelijke bijeenkomsten. Een aantekening hierbij is wel dat de meeste modems gebouwd worden rond dezelfde chipsets van een beperkt aantal fabrikanten (Broadcom, Intel, Texas Instruments, Scipio, Qualcomm); dit heeft tot gevolg dat vooral de verschillende chipsets tegen elkaar getest moeten worden.

Het is daarmee onwaarschijnlijk dat een fabrikant een standaard compliant modem op de markt brengt die toch niet wil samenwerken met de apparatuur van andere aanbieders. Wat wel mogelijk is, dat er opties zijn welke niet bij iedere fabrikant aanwezig zijn. In een dergelijk geval zullen de functies niet geactiveerd worden of zal de modem terugvallen naar een standaard of zelfs een lager modus. Mocht een modem om wat voor reden dan ook voor verstoringen zorgen in een signaal, dan zal de DSLAM of de CMTS als eerste de modem instrueren om een andere modus te kiezen, werkt dit niet, dan wordt de modem geïnstrueerd om terug te vallen op andere technieken, bv ADSL of Docsis 1.1 welke in een lager spectrum zitten. Mochten er nog steeds verstoringen zijn, dan kan de DSLAM of CMTS zelfs communicatie af sluiten. Een modem die geen werkende verbinding heeft zal in principe geen signalen sturen.²¹ Een en ander betekent dat er geen negatieve externe effecten te verwachten zijn van vrije modemkeuze op andere delen van het netwerk, waaronder de toegang tot het netwerk voor andere aansluitingen.

Uitzonderingen in Nederland niet waarschijnlijk

In Nederland is het zo dat sinds de introductie van nieuwere VDSL2 vormen, zoals bonded VDSL KPN als leverancier optreedt van overgrote meerderheid van de DSLAMs. Alternatieve aanbieders maken geen gebruik van eigen DSLAMs voor VDSL, maar soms nog wel voor ADSL. Dit heeft de markt voor ontbundelde local loop grotendeels veranderd naar een Managed Wholesale Broadband Access markt. Voor alternatieve aanbieders betekent dit dat zij geen "eigen" functies kunnen toevoegen, zoals de hierna genoemde NITRO optie. Een additioneel effect is

²¹ Een network engineer van een ISP verklaarde off-the-record tegen Stratix dat hij niet meegemaakt had dat een niet-compliant modem voor langdurige problemen zorgde. In een heel extreem geval zou het moedwillig kunnen, maar dat gold ook voor het zetten van 220V op de verbinding.

dat KPN goed moet specificeren welke eisen zij aan de apparatuur stelt. Deze gegevens zullen ook beschikbaar zijn voor fabrikanten om hun apparatuur op aan te passen.

In ADSL-gebaseerde netwerken was de performance van een verbinding alleen afhankelijk van de lengte van de lijn en de gebruikte chipset. Door overal dezelfde chipset te gebruiken met dezelfde instellingen kan de performance soms structureel worden verbeterd. Zo wist de Franse aanbieder Iliad/Free 28Mbit/s te halen door zowel in haar DSLAM als in de modem gebruik te maken van een Broadcom chipset²² waar de zogenaamde NITRO functie geactiveerd was. Zou een dergelijke modem in een ander netwerk geactiveerd worden, dan wordt deze functie niet geactiveerd.

In VDSL2 netwerken is het van belang dat er een bepaalde mate van coördinatie tussen de gebruikte profielen in een segment is. In VDSL2 wordt er gebruik gemaakt van active noise cancelling, waardoor er met het signaal ook een ander signaal meegezonden wordt, dat er op gericht is om de verwachte ruis op de lijn op te heffen door het exact tegengestelde signaal te verzenden. Het is mogelijk om twee verschillende profielen (bv 17a en 35 (vPlus)) naast elkaar te gebruiken.²³ Er is een uitzondering voor profielen 17 en 30a welke elk een andere spacing gebruiken en daardoor incompatibel zijn.²⁴ Modems worden door de DSLAM geïnstrueerd welke profielen gebruikt kunnen worden en zullen ingeval zij incompatibel zijn geïnstrueerd worden om terug te vallen naar ADSL.

In Nederlandse situatie is het op DSL-netwerken goed mogelijk om te specificeren wat de parameters zijn waar een VDSL-modem aan moet voldoen. Uit het onderzoek en de reacties van de aanbieders is ook gebleken dat KPN deze specificaties aan haar afnemers bekend maakt en een proces heeft om apparaten te testen. Het is voor een DSL operator ook mogelijk niet standaard modems te dwingen om alleen maar op 2,2 Mhz (ADSL) te functioneren. Ten aanzien van de geleverde internetsnelheden is het dan ook redelijk te verwachten dat een modem die aan de standaarden van de aanbieder voldoet, in staat is de geboden snelheden te leveren en dat als er een probleem is er een mechanisme is waardoor de modem terugschakelt in snelheid of zelfs in het geheel geen verbinding kan maken.

Om de vrije modemkeuze in een DSL-netwerk mogelijk te maken is het vooral van belang dat de technische parameters van het aanbod goed gespecificeerd worden. Als er fabrikant specifieke opties gebruikt worden, dan moet de aanbieder bekend maken wat de effecten zijn als deze opties niet geactiveerd zijn. Wordt zonder deze opties de verbinding in het geheel niet mogelijk, of is dan de maximale theoretische snelheid niet haalbaar etc.

Kabelnetwerken

In kabelnetwerken wordt voor breedband gebruik gemaakt van de Docsis standaard. Hiervan is de standaardisering in handen van CableLabs. Deze organisatie levert internationale standaarden, waar alle fabrikanten zich aan conformeren. VodafoneZiggo ondersteunt een veelheid van fabrikanten van modems in haar netwerk. Hier kan uit afgeleid worden dat haar netwerk

²² Voor een overzicht zie <http://www.journaldufreenaute.fr/29/08/2006/comment-fait-free-pour-proposer-les-meilleurs-debits-adsl-2-en-france.html>

²³ What is "35b supervectoring"? <https://en.avm.de/guide/high-speed-and-range/what-is-35b-supervectoring/>

²⁴ Vplus gets more out of VDSL2 vectoring <https://insight.nokia.com/vplus-gets-more-out-vdsl2-vectoring>

niet rond een bepaalde leverancier of implementatie gestandaardiseerd is. Daarbij staan de meeste kabelbedrijven alleen geregistreerde modems toe in hun netwerk. De MAC-adressen van deze modems moeten geactiveerd zijn, anders wordt er geen verbinding opgezet. Het argument dat een onbekende modem kan leiden tot verminderde performance lijkt dan ook vreemd. De uitleg dat een hele streng afgesloten moet worden ook. Het is waarschijnlijker dat als er een probleem is in het netwerk, als eerste gekeken wordt naar "vreemde" modems en die klant gebeld wordt. Als het niet deze modem is, dan zullen alle modems in een streng bekeken moeten worden, aangezien het dan ook om modems van de aanbieder gaat, is dit een normale situatie voor probleemoplossing.

Aangezien de aanbieders veelal geen uniform netwerk hebben, zullen ze sowieso naar een veelheid van modems moeten kijken. Ook in dit opzicht is er geen verandering voor de situatie van andere aansluitingen. De vrije modemkeuze zal als zodanig dan geen grote risico's met zich meebrengen. Wel zullen de aanbieders een administratief proces moeten inrichten om de modems van klanten te registreren en activeren in het netwerk.

Glasvezelnetwerken

In glasvezelnetwerken wordt er in Nederland vooral gebruik gemaakt van de Ethernet standaard. Deze standaard is internationaal zeer goed gestandaardiseerd. Het is de meest gebruikte standaard in wide area en local area networks. Er zijn echter wel verschillende smaken Ethernet, bijvoorbeeld ten aanzien van de te halen snelheid (1Gbit/s of 10Gbit/s) en multimode of singlemode glasvezel. In Nederland wordt vooral 1Gbit/s singlemode gebruikt. Aangezien iedere gebruiker hier een eigen verbinding los van andere gebruikers heeft kan er geen sprake zijn van onderlinge beïnvloeding. Er lijken technisch geen redenen te zijn waarom een Ethernet modem van een andere aanbieder niet zou samenwerken als beide einden dezelfde versie Ethernet en onderliggende transmissiestandaard ondersteunen. Een alternatieve techniek is xPON, waar een variant van is die waarbij eindgebruikers dezelfde glasvezelverbinding delen. Echter ook de xPON standaarden zijn goed gestandaardiseerd en al jaren beschikbaar. Verwacht mag dan ook worden dat ook deze apparaten met elkaar kunnen communiceren.²⁵ Mocht er onverhoopt een PON-modem in een Ethernet-netwerk gebruikt worden of vice versa, dan zullen de modem en de switch geen verbinding op kunnen zetten en niet kunnen communiceren. Het activeren van een Ethernet laser op een PON verbinding heeft wel tot gevolg dat tot ongeveer 64 gebruikers op een streng niet kunnen communiceren. Het is dus wel van belang dat er goede communicatie is richting gebruikers over wat voor aansluiting zij hebben.²⁶

In glasvezelnetwerken zullen aanbieders moeten specificeren wat voor techniek ze gebruiken, mogelijk enkele parameters en eventueel een operationeel proces inrichten om de modem te registreren.

Noodzaak van professionele ondersteuning niet evident

²⁵ Er zijn wel signalen dat de standaardisatie van PON minder solide is dan die van P2P glasvezel. Waar P2P veelal werkt, kunnen er bij PON meer mitsen en maren zijn.

²⁶ Dat deze communicatie niet altijd goed verloopt werd duidelijk toen het Stratix kantoor een upgrade van de glasvezelverbinding kreeg en de meegeleverde documentatie sprak van een GPON aansluiting. Dit terwijl de betreffende aanbieder volgens onze informatie nog geen GPON toepast.

Een aanbieder stelt ook nog dat het aansluiten op glasvezel alleen gedaan kan worden door professionele monteurs. Dit argument vindt echter weinig weerklank bij haar concurrenten, welke filmpjes online gezet hebben hoe de klant zelf een NTU/modem kan aansluiten.²⁷ Professionele installatie is nodig bij het correct aansluiten van een connector op het uiteinde van de binnenkomende glasvezel, en dit is zeker in de zakelijke markt met hogere snelheden en professionele SLA's belangrijk. De hierna beschreven koppelingen kunnen in de consumentenmarkt in principe door eindgebruikers gedaan worden.

Vanuit de aanbieders kwam ook het argument dat de glasvezelverbindingen ook wholesale inclusief een modem geleverd worden. Dit richt zich niet zozeer op de laag 1 tm 3 verbindingen naar het huis, maar meer op de operationele werkzaamheden (men zou kunnen zeggen de business-laag). Het klopt dat de netwerkaanbieder minder controle heeft over de verbinding en dus minder garanties kan geven. Dit zal echter ook bij de retail aanbieder en zijn klant bekend zijn. Als er dan problemen zijn, zal het vooral zaak zijn de operationele invulling van de ondersteuning van de klant goed vorm te geven, zodat de helpdesk van de aanbieder op de hoogte is. Ook de doorvertaling richting de meer technische tweede lijn zal goed ingericht dienen te zijn.

De vrije modemkeuze vereist in de consumentenmarkt geen professionele ondersteuning bij de installatie, noch hoeft het problematisch te zijn voor de kwaliteitsgaranties die afgegeven zijn aan gebruikers. In de zakelijke markt is aansluiten door professionals noodzakelijk en gebruikelijk.

Combineren 4G/DSL is mogelijk issue

Bij sommige oplossingen worden access technologieën gecombineerd (in Nederland vooral DSL/4G²⁸). Hiervoor is apparatuur bij de aanbieder en bij de klant nodig. Deze apparatuur kiest aan beide kanten welke fysieke verbindingen gekozen wordt voor het verkeer en voegt aan de andere kant het verkeer weer samen. Deze apparatuur aan de gebruikerskant is volgens aanbieders per definitie nog deel van het netwerk. Alhoewel aanbieders niet erg scheutig zijn met informatie over deze oplossingen, lijkt het dat de implementatie gebruik maakt van Multipath TCP²⁹ hetgeen gestandaardiseerd is in RFC 6824.³⁰ Het lijkt er wel op dat er geen uniforme implementatie van deze standaard is, omdat de implementaties veelal niet-interopeerbaar hoeven te zijn en de fabrikanten dus onderling niet testen of ze de standaard op dezelfde wijze geïmplementeerd hebben. Dit zou betekenen dat er mogelijk problemen kunnen ontstaan tussen implementaties van twee fabrikanten. Het is echter moeilijk dit in de praktijk te verifiëren. Een fabrikant die hier een product voor wil aanbieden zal een combinatie van

²⁷ http://www.fiber.nl/files/pdf/handleidingen/installatie/Doe-Het-Zelf_voor_Glasvezel.pdf

²⁸ Ook voor het combineren van Satelliet en vast zijn standaarden, maar deze worden in Nederland niet/nauwelijks gebruikt http://www.etsi.org/deliver/etsi_tr/103300_103399/103351/01.01.01_60/tr_103351v010101p.pdf

²⁹ Multipath TCP werkt ook alleen maar voor TCP als protocol. Niet alle communicatie op het Internet is TCP. Sommige VPN protocollen werken met UDP en profiteren niet van het combineren van 4G en DSL. Het modem kiest dan een van de beschikbare paden en combineert ze niet beide. Multipath TCP vergt ook dat er aan de andere kant (bij de aanbieder) een oplossing in het netwerk staat dat de TCP verbindingen samenvoegt. Multipath TCP wordt ook door Apple gebruikt om de performance van Siri te verbeteren. Hier kiezen de servers van Apple en de telefoon welke breedband verbinding (wifi of 4G) ze kiezen voor de communicatie.

³⁰

gestandaardiseerd DSL met gestandaardiseerd 4G moeten aanbieden waarover de door de aanbieder gebruikte variant van RFC 6824 is ingezet. Een oplossing voor de mogelijke incompatibiliteit is om net als bij andere standaarden plugfests te organiseren in de standaardisatie-organisaties.

De aanbieders zullen in dit geval goed moeten specificeren hoe zijn Multipath TCP geconfigureerd hebben, zodat andere fabrikanten apparatuur kunnen maken die hiermee kan samenwerken. Naast een specificatie is het ook nodig om de gebruiker van een a-kaart te voorzien welke voor het 4G netwerk gebruikt kan worden. De nummers behorende bij de SIM-kaart en de DSL-aansluiting zullen ook in de administratie van de aanbieder geregistreerd moeten worden.

Bridge modus ondersteuning nu niet overal gebruikelijk

Vanuit de gebruikers komt de suggestie om in ieder geval altijd een bridge modus te ondersteunen. Dit is een variant waarbij de modem alleen maar als modem functioneert. Functies als firewall, network address translation etc. worden allemaal uitgezet. Het modem functioneert dan zuiver als modem en handelt laag 1 en 2 af. Alle authenticatie (protocollen als PPP, etc.) worden doorgegeven aan het volgende apparaat. Op deze wijze kan een goed geconfigureerde switch/router zelf het netwerk beheren in plaats van de door de ISP geleverde modem. Deze mogelijkheid wordt door VodafoneZiggo wel ondersteund, maar door KPN niet op alle modems. Andere aanbieders bieden deze mogelijkheid veelal ook. Het aanbieden van Bridge Mode werkt niet op verbindingen die gebruik maken van Multipath TCP. Dit omdat er in de router een multipath verbinding opgezet wordt.

Het activeren van bridge mode betekent niet dat de gebruiker een vrije keuze van modem heeft. Het effect is wel dat de gebruiker zelf kan bepalen wat voor router deze wil gebruiken. De router zal ook alle door de aanbieder gebruikte functionaliteit moeten ondersteunen. Een voorbeeld is bijvoorbeeld Multicast, wat niet altijd door routers (Bv mesh wifi routers) ondersteund wordt.

Conclusies impact operator netwerk

De meeste aanbieders gebruiken gestandaardiseerde technologieën voor het ontsluiten van hun klanten. Dit betekent in de praktijk dat ook modems van andere merken zouden moeten werken met hun aanbod. Vrije modemkeuze zal dan ook geen of weinig effect op het technisch functioneren van de netwerken hebben. Wel zullen bedrijven operationele processen moet inrichten voor modemregistratie en ondersteuning van klanten.

Voor het combineren van 4G en DSL kunnen er op dit moment wel praktische problemen zijn, omdat, ondanks dat de onderliggende netwerken gestandaardiseerd zijn, de wijze waarop MPTCP gebruikt wordt niet goed gestandaardiseerd kan zijn. Dit is echter meer het gevolg van een gebrek aan samenwerking rond standaardisatie, dan een fundamentele eigenschap van de techniek. Vermits aanbieders publiceren op welke wijze zij hiervan gebruik maken, zal het ook voor anderen mogelijk zijn om hier werkende implementaties voor te bouwen³¹. Ook zullen

³¹ Maar het ontwikkelen en verkopen van alternatieve werkende implementaties is natuurlijk vooral interessant als er voldoende afzetmarkt is. Voldoende standaardisatie speelt hierbij een belangrijke rol.

aanbieders een proces moeten inrichten waarbij consumenten toegang krijgen tot SIM-kaarten en deze kunnen activeren voor de dienst.

5.2 Issues rond impact op Veiligheid

5.2.1 Belangrijkste effecten

De volgende effecten worden in de consultatiereacties beschreven:

- *Algemeen veiligheid:* Zorgen over gevolgen voor veiligheid en continuïteit van beleidsregel (angst dat dit eerder negatief dan positief uitpakt).
- *Verkeerde instellingen:* Klant kan verkeerde instellingen gebruiken. Communicatie daarover met aanbieder is moeilijk als het een door de klant aangeschaft apparaat betreft. Ondersteuning vele verschillende typen modems is lastig, leidt mogelijk tot meer storingen. Verantwoordelijkheid is onduidelijk.
- *Certificering:* Certificering van losse modems / routers etc. nodig.
- *Verstrekken gegevens aan klanten:* Operators dienen identificatie, authenticatie en/of beveiligingsfunctie gegevens te verstrekken aan abonnees.
- *Firewall bij operator laten:* Veel consumenten snappen veiligheidsissues niet, daarom firewall bij operator laten.
- *Diversiteit is veiligheid:* Meer diversiteit van modems maakt het voor kwaadwillenden juist lastiger om een zwak punt grootschalig te exploiteren.
- *Onderhoud modems kan leiden tot onveiligheid:* Onderhoud van modems die niet door de provider ter beschikking worden gesteld kan geen verplichting zijn voor een operator. Dit geeft risico's op het gebied van internetveiligheid.

Veiligheid is een belangrijk thema in de reacties. Vooral aan de kant van de aanbieders wordt er gewezen op mogelijke problemen met de veiligheid van de modems, maar ook met het netwerk van de klant. Dit is niet onterecht aangezien de moderne modems volledige computeromgevingen zijn waarin een veelheid van functies uitgevoerd worden. Naast een modem, switch, firewall, access point en router bevat het apparaat een webserver voor de configuratie, en soms nog andere functionaliteiten als fileserver en printserver. Slecht gepatchte of beveiligde en gehackte modems hebben in het verleden ook voor veel problemen gezorgd³². Veiligheid kan opgesplitst worden in 3 delen:

- Veiligheid van de modem zelf.
- Veiligheid van het netwerk van de klant achter de modem.
- Veiligheid van de rest van het Internet als gevolg van de onveiligheid van de modem of het netwerk van de klant.

³² Een voorbeeld is het Mirai botnet. Dit maakte gebruik van gehackte routers, maar veroorzaakte ook problemen in de modems van verschillende ISPs. <https://blog.cloudflare.com/inside-mirai-the-infamous-iot-botnet-a-retrospective-analysis/>

5.2.2 Validatie van de technologische argumenten

Opvallend is dat in de reacties de aanbieders de vrije modemkeuze vooral zien als een beveiligingsprobleem, terwijl de gebruikers juist de bijdrage van vrije modemkeuze aan ICT-veiligheid noemen.

Wat betreft de veiligheid van de modem zelf wijzen aanbieders er op dat er geen garanties zijn dat de modems die de gebruikers aanschaffen voldoen aan de veiligheidseisen die zij stellen ten aanzien van modems, om deze modems zelf te beschermen en ook het netwerk van de klant dat er achter ligt. Van de kant van de gebruikers wordt echter gewezen op een aantal gevallen waarin de modem van de operator niet of niet snel voldoet aan veiligheidseisen.

In de praktijk is de situatie echter complexer. Er is bijna geen ISP die zelfstandig verantwoordelijk is voor de ontwikkeling van de hardware en de software die zij leveren aan klanten. Zij kopen deze veelal in bij een aantal leveranciers. Wat het nog complexer kan maken is, dat de modems zelf veelal gebouwd zijn rond de chipsets van een beperkt aantal fabrikanten. De modems die door consumenten gekocht kunnen worden zijn veelal op basis van dezelfde of vergelijkbare chipsets gebouwd. Op deze modems draaien vaak specifieke varianten van open source software zoals Linux en daaroverheen weer andere veelgebruikte open en closed source software of eigen applicaties. De software implementeert weer verschillende publieke en bedrijfseigen standaarden en soms ook nog specifieke oplossingen van de ISP. In elk van deze lagen kan een security probleem zitten waar gebruikers last van kunnen hebben. En in de afgelopen jaren is meermalen bewezen dat fouten in hardware, software, standaarden en operator implementaties van deze veiligheidsproblemen kunnen zitten.

Een bekend recent probleem zat in opeenvolgende generaties van de Puma 5, 6 en 7 processoren van Intel voor kabelmodems. Deze zijn de basis zijn van kabelmodems van Comcast, Virgin UK en VodafoneZiggo. Deze processoren hadden een probleem waardoor de latency van pakketten zeer hoog kon worden³³. Dit effect trad al op bij dagelijks gebruik en leidde tot veel klachten van eindgebruikers. Alhoewel de basis van het probleem al in 2016 gedocumenteerd was, werd de volle omvang ervan in 2017 wereldwijd duidelijk. Vanuit veiligheidsoogpunt is relevant dat al in april 2017 bekend werd dat een stroom pakketten van ongeveer 200kbps in principe in staat was om een kabelmodem onbereikbaar te maken. Het effect is een zogenaamde "Denial of Service"-attack. VodafoneZiggo verwachtte pas in april 2018 een patch te kunnen hebben.

Deze casus laat goed zien hoe complex de ketens zijn voor de levering van een internettoegangsdienst. Het probleem zat in chips van Intel, die geleverd werden aan veel modem fabrikanten. Intel dient het probleem te beschrijven en waarschijnlijk ook software aan te passen en dit aan haar klanten, de modemfabrikanten, te zenden. Deze modem fabrikanten dienen hun software aan te passen. Soms dienen de fabrikanten ook nog specifieke wijzigingen te maken voor bepaalde ISPs. Daarna worden de wijzigingen getest door ISPs en uiteindelijk uitgerold naar de eindgebruiker. Probleem voor veel kabelgebruikers wereldwijd was dat hun ISP hen niet toestond om een andere modem te gebruiken, en enkele kabelaanbieders volledig op deze 3 generaties Intel chips gestandaardiseerd waren, dus een up of downgrade had geen

³³ Voor achtergrond zie oa https://www.theregister.co.uk/2016/12/03/intel_puma_chipset_firmware_fix/

effect. Ziggo-gebruikers adviseerden elkaar op discussieforums als Tweakers om over te stappen naar een andere modem, zonder Intel chipset.

Deze casus laat zien, dat bugs voor kunnen komen bij de grootste en meest gerenommeerde leveranciers. Het laat ook zien dat ISPs niet een betere of slechtere onderhandelingspositie hebben dan consumenten om bugs gerepareerd te krijgen. Als hun leverancier het niet snel repareert, dan zullen zij moeten wachten. Problematisch voor hen is wel, dat ze vaak door contracten, interne procedures, etc. niet eenvoudig (met een paar honderdduizend modems) over kunnen stappen van leverancier. Dit in tegenstelling tot individuele gebruikers, die in principe bij een leverancier een modem van een andere leverancier kunnen aanschaffen. In dit geval ging het om een mogelijk DDos probleem, wat alleen de gebruiker zonder verbinding laat.

Echter er zijn andere gevallen bekend waarbij hackers de DNS instellingen van miljoenen Braziliaanse modems aanpasten³⁴, zodat ze onopgemerkt passwords, creditcard gegevens, etc. konden stelen en miljoenen buit maakten. Op eenzelfde wijze zijn modems misbruikt om *netwerken buiten het netwerk van de klant* of ISP aan te vallen middels DDOS of andere vormen van aanvallen.

Het idee zou misschien kunnen ontstaan dat dit probleem alleen bij ISPs bestaat, maar dezelfde modems die ISPs kopen zijn veelal ook voor *consumenten* te koop. Het is dus niet gezegd dat de een of de andere beter is.³⁵ Beide partijen maken ook vergelijkbare afwegingen tussen kosten en functionaliteit. Beide proberen de beste functionaliteiten te kiezen met de laagste investering vooraf en de laagste kosten over de levensduur van de modem. Daarnaast zijn er ook meer op consumenten gerichte fabrikanten en deze hebben geen betere reputatie. Zo klaagde de Amerikaanse FTC recent een fabrikant van routers aan wegens het bewust niet updaten van lekke routers. Andere fabrikanten patchen alleen routers die aan hen gemeld worden als lek, niet alle routers waar de software in zit. Soms moeten consumenten zelf patches uitvoeren, maar worden niet geïnformeerd over problemen en de gevolgen als ze niets doen. De veiligheid van een aansluiting zal afhangen van de situatie. Zijn er problemen in de modems van de ISP, dan zal een kleine groep goed geïnformeerde klanten besluiten om een andere oplossing te kiezen, maar een groot deel van de klanten blijft met het probleem zitten. Andersom als er een probleem zit in een modem die door een kleine groep klanten gekocht is, dan zijn deze klanten en hun ISP afhankelijk van de snelheid waarmee de fabrikant de problemen oplost. Mocht de ISP last krijgen van deze modems, omdat ze bijvoorbeeld opgenomen zijn in een botnet, dan kan de ISP maatregelen nemen tegen deze modems.

Configuratie en misconfiguratie is hoe dan ook een aandachtspunt

Ten aanzien van *configuraties* en misconfiguraties is het waar dat het mogelijk is dat consumenten de verkeerde instellingen activeren in hun modem/routers. Dit probleem is altijd aanwezig. Goede communicatie vanuit de operator is hiervoor van groot belang. Nu worden deze

³⁴ Sophos geeft hier een overzicht van de Braziliaanse situatie <https://nakedsecurity.sophos.com/2012/10/01/hacked-routers-brazil-vb2012/>

³⁵ Een chronologisch overzicht van allerlei modem/router problemen bij een veelheid van fabrikanten kan gevonden worden op deze site <https://routersecurity.org/bugs.php>. De toon is enigszins gefrustreerd te noemen, maar wel begrijpelijk gezien de niet aflatende stroom problemen. Andere pagina's laten zien hoe de onveiligheid van routers/modems misbruikt wordt.

gegevens en eventuele gevolgen niet altijd goed gecommuniceerd, zelfs al kan de consument wel wijzigingen maken in de modem/router van de ISP. Het is daarmee onduidelijk of een vrije routerkeuze leidt tot meer problemen met misconfiguraties, aangezien het ook een stimulans zal zijn om beter te communiceren over instellingen. Voor zover misconfiguraties leiden tot slecht functionerende modems wordt verwezen naar de voorgaande analyse ten aanzien van de effecten hiervan op het netwerk en andere gebruikers.

Firewall beheer operators heeft op dit moment niet veel meerwaarde

Een suggestie was om de *veiligheid van het netwerk van de klant* te verhogen door het beheer van de *firewall* bij de operator te laten. Problematisch bij deze stelling is dat de modems zoals geleverd door aanbieders op dit moment wel een firewall bevatten, maar dat deze firewall in de praktijk weinig doet en ook weinig functionaliteit heeft. Zo bevat de firewall van de KPN Experia box geen regels welke de veiligheid van het netwerk verhogen. De meeste aanbieders bieden ook geen URL-filtering, kinderfilters, etc. in hun apparaten aan. Recent heeft XS4All wel een dienst geactiveerd, maar deze werkt via haar DNS server en bevindt zich dus buiten het thuisnetwerk.³⁶ Veel verder kan een ISP ook niet gaan, zonder actief kennis te nemen van de inhoud van communicatie of verkeer te blokkeren. Nog afgezien dat dit technisch moeilijk is en waarschijnlijk meer stuk maakt dan het oplost, stellen ook regels rond privacy en net-neutraliteit beperkingen aan deze oplossing. Wil een klant wel dienstverlening die het internetgebruik veiliger maakt, dan zal deze een andere router moeten aanschaffen, waar dit soort diensten ingebouwd zitten. Het inbouwen van deze functies is een trend die meer zichtbaar is in de consumentenmarkt, dan in de markt die zich richt op ISPs.

5.2.3 Conclusies impact veiligheid

De conclusie van deze paragraaf is toch, dat er zorgen kunnen zijn rond de beveiliging van modems en routers, maar dat de vrije modemkeuze daar geen fundamentele veranderingen in brengt. Het maakt hierbij niet uit of deze door de ISP geleverd of door de klant zelf gekocht zijn. Veel problemen ontstaan bij de fabrikant en de ISP en de eindgebruiker zijn beide klant. In sommige gevallen zal de ISP beter zijn in het bestrijden van veiligheidsproblemen, in andere gevallen kan de consument beter zijn. De problematiek verandert echter niet. Het toestaan van diversiteit in het netwerk kan in ieder geval consumenten de mogelijkheid geven om een modem/router om te wisselen in geval de problemen aanhouden. Hiervoor is het wel nodig dat er duidelijkheid is over de oorsprong van het probleem, zodat niet een ander apparaat met dezelfde problemen gekocht wordt.

5.3 Issues rond impact op diensten

5.3.1 Belangrijkste effecten

De reacties geven ook meningen over de effecten die er mogelijk kunnen zijn op de wijze waarop diensten worden aangeboden aan eindgebruikers. Een aantal argumenten komen naar voren:

³⁶ XS4ALL introduceert als eerste provider malwarefilter in netwerk, 24 April 2018, <https://blog.xs4all.nl/xs4all-introduceert-als-eerste-provider-malwarefilter-in-netwerk/>

- Ten aanzien van televisie wordt gesteld dat dit niet mogelijk zou zijn als de aanbieders niet hun eigen set-top boxen kunnen leveren. Argumenten hiervoor zijn de noodzaak voor Digital Rights Management mede vanuit de content eigenaren en de noodzaak om nieuwe functies toe te kunnen voegen. Enkele consumenten noemen daarentegen bezwaren tegen DRM.
- Voor IP-telefonie zit de beveiliging in de modems en deze kan niet losgekoppeld worden.
- Overige diensten als publieke wifi kunnen alleen aangeboden worden door gebruik te maken van de modem/router van de aanbieder.
- In de zakelijke markt zijn garanties ten aanzien van beschikbaarheid, redundantie en te behalen performance vaak een onderdeel van de dienst. Aanbieders zijn van mening dat zij met deze regels gedwongen kunnen worden om deze garanties te leveren op apparaten waar zij geen controle over hebben.

5.3.2 Validatie van de technologische argumenten

De argumenten van de aanbieders volgen het stramien, dat omdat het nu zo is, kan het niet anders. Maar wat als het anders moet? Wat als de regels zo zijn, dat eindgebruikers hun eigen eindapparaten kunnen kiezen en koppelen?

Ondersteuning 'basisdiensten' zoals TV en telefonie kan anders: Over veel DSL- en FTTH netwerken wordt IP-TV gebruikt voor het verspreiden van TV content³⁷. Om dit te kunnen decoderen en om alle bijbehorende functies (opnemen, on-demand, etc.) te gebruiken heeft de consument een set-top box in huis. Deze box wordt door de ISP aangeleverd. In dit onderzoek wordt aangenomen dat deze diensten ook onder de scope van de beleidsregel vallen. Dat betekent dat als een aanbieder een eigen STB meeleverd bij de dienst televisie als integraal onderdeel van zijn dienst, de klant ook de mogelijkheid moet hebben om een ander apparaat te gebruiken (van een andere fabrikant of zelfgebouwd middels open source software³⁸).

De vraag kan gesteld worden of IP-TV wel kan functioneren zonder controle van de ISP over de modem en STB. Aan de netwerk kant blijkt het goed mogelijk te zijn om eigen apparatuur in te richten. Het vergt enige configuratie van de eindgebruiker, want IPTV van bijvoorbeeld KPN gebruikt multicast als onderliggende techniek en een apart VLAN. Hiervoor dient de modem/switch/router geconfigureerd te worden om te kunnen functioneren met (multicast) VLANs. Bijvoorbeeld de informatie op de website netwerkje.com laat zien dat dit goed mogelijk is. Deze website geeft ook nog wat achtergrond ten aanzien van de routing van IPTV:

Van oudsher gebruikt KPN de zogenaamde "bridged IPTV" methode om IPTV aan te bieden. Hierbij vormt de Experiabox slechts een brug tussen de decoders en het IPTV netwerk, maar voegt verder geen functionaliteit toe. De decoders zitten op hun eigen netwerk, los van het netwerk thuis gescheiden door VLANs.

³⁷ Bij een deel van de kleinere FTTH-aanbieders, vooral die met een historie als CATV aanbieder wordt het TV-signaal nog als een traditioneel kabel signaal op de Coax aansluiting in huis gezet.

³⁸ Zo is er een grote community rond XMBC ook wel bekend als Kodi. Dit is op zijn beurt weer de basis van bv het Horizon platform van Liberty Global

Sinds 2015 stapt KPN over op "routed IPTV" waarbij de IPTV decoders wel een onderdeel vormen van het thuis netwerk, daarom ook een IP adres krijgen van de Experiabox in dezelfde range als alle andere apparaten en waarbij de routing naar het IPTV netwerk ook door de Experiabox gedaan wordt. De integratie met het thuisnetwerk en het internet biedt mogelijkheden voor nieuwe functionaliteiten zoals de integratie met Netflix.

Hieruit kan geconcludeerd worden dat de STB van KPN in technische zin onderdeel uit maakt van het thuisnetwerk van de gebruiker. Het is echter wel zo dat de router/switches in huis het gebruik van multicast VLANs moeten kunnen ondersteunen. Zo werken bijvoorbeeld veel mesh-Wifi oplossingen niet met multicast VLANs.³⁹

Set top box

Rond de STB ontstaan wel complexere situaties. De STB is in essentie niets anders dan een computer met een processor, grafische kaart, een operating systeem en een aantal programma's er op, welke verschillende vormen van TV afspelen, opnemen, kopen, etc. mogelijk maken. Tot voor een paar jaar geleden waren STBs specifiek voor een fabrikant of zelfs een telecombedrijf. Er zijn ontwikkelingen die er op wijzen dat de markt voor STBs die van de televisie en smartphone volgt, met vergelijkbare chipsets en besturingssystemen. Android TV en Apple TV worden soms al op deze wijze ingezet.⁴⁰ Dit maakt het mogelijk voor telecombedrijven om de apps die ze voor tablets en smartphones ontwikkelen geheel of gedeeltelijk te hergebruiken voor STBs. Wil een fabrikant een concurrerende STB in de markt zetten, dan zal deze de combinatie van hardware, software, DRM en andere functionaliteit moeten ondersteunen, welke functioneel tot een diep niveau niet te onderscheiden is van die van de aanbieder.

Als de consument zelf een set top box moet kunnen kiezen, dan is de eerste vraag hoeveel van de functionaliteit ondersteund moet kunnen worden. Als het alleen gaat om het en selecteren en bekijken van televisiestreams over IPTV of kabel dan lijkt dat nog wel mogelijk. Op een kabelnetwerk worden de belangrijkste kanalen altijd uitgezonden en kunnen andere kanalen op verzoek bijgeschakeld worden. Hiervoor zijn standaarden beschikbaar. Ook voor IPTV geldt ook dat het activeren van een stream een standaard volgt. Het kijken van traditionele lineaire televisie lijkt dus mogelijk en te ondersteunen, mits IPTV aanbieders publiceren welke standaarden ze gebruiken en hoe deze geïmplementeerd zijn.

Er ontstaat wel een probleem met Digital Rights Management (DRM). Deze DRM is veelal gekoppeld aan hardware. Dit kan in een door de provider geleverde STB geïntegreerd zijn, maar kan ook middels een smartcard. Daarbij moet de DRM ook ondersteund worden vanuit de software en de DRM-fabrikanten ondersteunen soms niet alle platformen. Deze DRM is nodig als de content aanbieder eisen dat de aanbieder van de televisiedienst maatregelen neemt tegen ongeautoriseerde toegang, opname en heruitzending van de content. Aangezien het

³⁹ Mesh-systeem voor beter wifi: 9 mesh-systemen getest, Marco den Teuling, C'T magazine - 6 maart 2018 <https://www.ct.nl/reviews/hardware/mesh-systeem-wifi-dekking-test/20692/>

⁴⁰ Voorbeelden van opertors die AppleTV inzetten als vervanging voor de set top box zijn bijvoorbeeld Salt.ch in Zwitserland en Canal+ in Frankrijk, zie <https://www.broadbandtv-news.com/2018/06/05/apple-tv-to-replace-traditional-cable-set-top-boxes/> en <https://resources.irdeto.com/home-page/will-android-kill-middleware-as-we-know-it>

gaat om een dienst die over het netwerk geleverd wordt, is er een grotere vrijheid van hoe de aanbieder dit invult. Dat niet alle hardware of software ondersteund wordt voor een televisie-achtige dienst is niet ongebruikelijk en speelt ook bij online diensten als Netflix. Ook hier speelt een combinatie van DRM en ondersteuning van applicatiefunctionaliteiten een rol. Zo kwamen gebruikers van oudere Philips Tv's er achter dat de Netflix ondersteuning voor hun TV eindigde.⁴¹ Traditionele kabelbedrijven hebben vaak een mogelijkheid voor op smartcard gebaseerde DRM systemen voor gebruik in televisies zonder STB⁴². Dit geldt niet voor IPTV gebaseerde opties. Deze zijn veel minder op openbare standaarden gebouwd en daarom zal er veelal eerst software op de TV geïnstalleerd moeten worden.⁴³

Vanuit de kant van de consumenten wordt opgemerkt dat zij bezwaren zien tegen het gebruik van DRM. Zonder DRM zou de implementatie van een andere STB of mediaplayer software zeker eenvoudiger zijn. De rechthebbenden op de content stellen het gebruik van DRM echter verplicht. In dit document gaan we niet verder in op dat debat en wordt ervan uit gegaan dat DRM noodzakelijk is.

Dat zelfs standaarden niet tot een eenduidige implementatie leiden is ook zichtbaar in de Nederlandse markt. Additionele functionaliteiten, zoals opnemen, terugspoelen begin gemist etc. zijn bij VodafoneZiggo ook via een CI+ 1.3 module beschikbaar, maar alleen in voormalig Ziggo gebied en niet in voormalig UPC gebied. Let wel, alleen 2 door VodafoneZiggo aangeboden CI+-modules worden ondersteund. Wil een gebruiker echter zowel kijken als opnemen, dan kan het zo zijn dat er twee CI+ modules nodig zijn; 1 voor de tuner die kijkt en 1 voor de tuner die opneemt. In voormalig UPC-gebied is de Horizon STB benodigd voor opnemen, terugspoelen etc. Bij KPN gebeurt het opnemen niet op de STB, maar op een centrale server. Een fabrikant van een alternatieve STB zal dus rekening moeten houden met verschillende opties, zelfs als het om 1 aanbieder gaat.

Om de additionele functionaliteiten werkend te krijgen zal een aanbieder meer moeten publiceren dan alleen de gebruikte standaarden. De aanbieder zal vrij diep inzicht moeten geven in de wijze waarop de software op de STB samenwerkt met de software op de centrale servers. Elke vorm van communicatie, elke call naar een API, elke library zal beschreven en gedefinieerd moeten worden. Hierbij moet niet alleen gedacht worden aan het opnemen en afspelen van content, maar ook opties voor ouderlijk toezicht, het blokkeren van zenders, mogelijk maken of voorkomen dat betaalde content gekeken kan worden etc. Ook zullen wijzigingen gecommuniceerd moeten worden. Dit is geen eenvoudig proces, want de combinaties van hardware en software kunnen effecten geven die niet optreden bij andere combinaties. Zo bleek bij de introductie van 4K op het KPN netwerk dat dit niet voor alle gebruikers vlekkeloos verliep en dat er patches nodig waren in de software. Daarbij waren de problemen vooral aanwezig bij bepaalde merken Tv's. Het kan zijn dat die patches alleen maar de werking van de STB veranderen, maar er kunnen ook patches zijn die de parameters van de communicatie wijzigen. De aanbieder zal dus niet kunnen volstaan met communicatie over parameters en

⁴¹ De gebruikers kregen nog wel een alternatief als compensatie <https://www.rtlnieuws.nl/technieuws/heb-je-een-oude-smart-tv-van-philips-dan-krijg-je-een-compensatie>

⁴² Zie onder andere bij Ziggo <https://www.ziggo.nl/televisie/mediaboxen/ci-plus/>

⁴³ Zie bijvoorbeeld <https://www.nevron.eu/blog/iptv-set-top-box/> waar een fabrikant het verschil uitlegd.

protocollen, maar inzicht moeten geven in de inhoud van bugfixes. Dit zal het complex maken voor een buitenstaander om een STB te ontwikkelen die, met andere hardware en software, toch op een zelfde manier werkt.⁴⁴ In feite wat er gepoogd wordt is om de STB van een aanbieder te reverse engineeren. Het construeren van een STB zal echter een zaak zijn voor de fabrikant, niet voor de telecomaangebieder zelf.

De telecomaangebieder kan er bijvoorbeeld voor kiezen gebruik te maken van smartcards. Zoals reeds beschreven wordt dit in de huidige praktijk soms toegepast. Dit kan de complexiteit ten aanzien van DRM voor de telecomaangebieder verminderen omdat deze apparatuur reeds aanzienlijk is gestandaardiseerd. Dit geldt ook voor andere identificatiesystemen zoals SIM-kaarten maar ook softwarematige identificatiemogelijkheden binnen bijvoorbeeld apps zijn mogelijk. Het zou vanuit een praktisch oogpunt ook eenvoudiger kunnen zijn als de aanbieder zijn STB software als een app beschikbaar maakt, zodat deze op andere STBs gedraaid kan worden (vergelijk met de Netflix app). Een eerste probleem is dan wel dat niet elke STB hetzelfde operating systeem draait. Linux (verschillende varianten), Android (Linux-gebaseerd) en iOS (AppleTV) zijn veel voorkomend. Aangezien AppleTV een gesloten systeem is kan een andere fabrikant hier geen alternatief voor aanbieden. Voor Android en Linux kan dit wel. Zeker voor Linux en in bepaalde mate ook voor Android moet dan wel de juiste versie met de correcte kernel en libraries gebruikt worden. Het kiezen van andere hardware kan dan al problemen met de app software veroorzaken. Een app als Netflix draait op zich op een veelheid van systemen, maar er is een heel team dat allerlei mogelijk versies test en op verschillende hardware probeert problemen op te lossen.⁴⁵ De vraag is dan vooral wat de motivatie zou zijn voor een ISP om zijn IPTV platform beschikbaar te stellen middels een app. Deze reden zou kunnen zijn, dat dit de uitrol van hardware bespaart. Hoe dan ook, het beschikbaar stellen van content via een app is reeds een zichtbare marktontwikkeling bij telecomaanbieders. Hier besproken regels kunnen echter wel een versnelling van deze marktontwikkeling naar over-the-top aanbod van content teweeg brengen. Als de app van de aanbieder namelijk volledig over-the-top werkt, dan is er aanleiding om aan te nemen dat deze niet onder de reikwijdte van de regelgeving valt. Dit zou tot effect kunnen hebben dat de TV-dienstverlening los is van het onderliggende netwerk. Dit zou er zelfs toe kunnen leiden dat er meerdere concurrerende OTT-televisiediensten in de markt komen.

Conclusie voor Set top Boxen (STBs)

Het openen van STBs is complex, niet alleen voor de fabrikant die een alternatief wil bieden voor een STB van een ISP en daarbij een complexe interface na moet bouwen, maar ook voor de ISP zelf. Het bekend maken van alle specificaties en deze bij iedere iteratie van de ontwikkeling documenteren is complex en zal een grote extra hoeveelheid administratie en consistentie vragen van de ontwikkelaars. Het is mogelijk dat aanbieders zullen opteren voor een OTT-aanbod om deze uitleg van de regelgeving te ontduiken. Dit zou er zelfs toe kunnen leiden dat er meerdere concurrerende OTT-televisiediensten in de markt komen.

⁴⁴ <https://forum.kpn.com/interactieve-tv-11/het-leed-dat-kpn-4k-heet-436751>

⁴⁵ Voor inzicht in de Netflix test infrastructuur zie <https://medium.com/netflix-techblog/automated-testing-on-devices-fc5a39f47e24>

Voice diensten

IP-Telefonie is een andere reden die genoemd wordt waarom een vrije modemkeuze niet mogelijk is. Bij KPN, VodafoneZiggo en Caiway is het niet mogelijk voor consumenten om zonder tussenkomst van de door KPN of VodafoneZiggo geleverde modem/routers een eigen VoIP telefoon te verbinden met de VoIP-servers van deze partijen. Ook bij andere ISPs is dit het geval. Klanten prikken een traditionele telefoon in de modem en de modem vertaalt de signalen naar VoIP commando's en een spraaksignaal. Het is in theorie ook mogelijk om een eigen VoIP telefoon aan te sluiten, maar dit wordt niet (meer) ondersteund door verschillende aanbieders. XS4ALL is hier een bekende uitzondering op. Telfort klanten met een oud-abonnement en bijbehorende oude modem kunnen ook nog hun eigen apparatuur aansluiten. Een paar kleinere ISPs, zoals Tweak, staan dit ook toe.

Bij KPN was er in het verleden wel een mogelijkheid om eigen VoIP telefoons aan te sluiten. De klant kon een verbinding maken met de interne SIP-server van de modem. Dit maakte het mogelijk om eigen VoIP-telefoons of zelfs een mobiele telefoon met deze SIP-server te verbinden. Deze mogelijkheid is later verwijderd. Uit discussies op het KPN-Forum blijkt dat de reden hiervoor was, dat dat ingebouwde SIP-server slecht beveiligd was en bijvoorbeeld gebruikt kon worden om twee gesprekken tegelijk te voeren (maar voor maar 1 gesprek te betalen). De SIP-server zit nog steeds in de modem, maar is nu alleen nog maar toegankelijk voor telefoons die rechtstreeks op de Experiabox zijn aangesloten.⁴⁶

XS4ALL is een voorbeeld van een aanbieder die haar klanten wel toegang geeft tot haar VoIP-server. Deze server bevindt zich op sip.xs4all.nl. Klanten van XS4ALL kunnen dus op elk apparaat met een VoIP-client verbinding maken met de telefoondienst. De klant is niet gebonden aan een modem of een daarin gebouwde SIP-server. Dit betekent wel, dat als de klant niet gebruik maakt van de modem van XS4ALL, de klant zelf een oplossing moet vinden om een traditionele telefoon aan te sluiten en de instellingen van de SIP-server in te voeren.

De aanbieders in de consumentenmarkt maken geen of beperkt gebruik van versleuteling tussen de modem en de SIP-server van de communicatie. In de zakelijke markt wordt soms wel gebruik gemaakt van Transport Layer Security (TLS). Hiervoor worden geen hardware gebaseerde versleutelingen of authenticaties (zoals een SIM-kaart) gebruikt. Dat betekent dat deze ook niet vervangen hoeven te worden.

Voor de authenticatie wordt wel gebruik gemaakt van encryptie. Het is om deze reden dat consumenten niet in staat geweest zijn om de login van het netwerk te "sniffen", door het verkeer tussen modem en het netwerk te tappen. Daarbij koppelen de aanbieders deze gegevens aan een bepaalde modem en lijn. Op deze wijze is het organisatorisch en technisch geborgd dat er geen misbruik van de VoIP-verbinding gemaakt kan worden.

Een aanbieder heeft gedetailleerd uitgewerkt wat dit voor haar bedrijfsprocessen betekent. Belangrijkste conclusie is dat het vooral werkzaamheden oplevert om de sleutels uit te wisselen en om de consument te beschermen tegen gehackte VoIP-telefoons en de gevolgen (bv

⁴⁶ <https://forum.kpn.com/vast-bellen-13/voip-toestel-kan-zich-niet-meer-aanmelden-op-experiabox-369503>

torenhoge rekeningen) hiervan⁴⁷. Mochten aanbieders verplicht worden om consumenten de mogelijkheid te geven hun eigen apparaten te gebruiken voor een VoIP verbinding, dan zal dit of:

- Gekoppeld blijven aan de bestaande verbinding en adres. Dit betekent dat de SIP-server alleen maar bereikt kan worden vanaf het thuisadres van de eindgebruiker.
- Een losse SIP-verbinding, op een vergelijkbare wijze gebeuren als nu bij XS4ALL het geval is, welke werkt op elk apparaat en elk netwerk. Dit is nomadisch gebruik.

Vanuit een deel van de aanbieders gezien zal het vooral problematisch zijn, dat zij op dit moment een gesloten systeem hebben. De klant gebruikt een apparaat aangeboden en beheerd door de aanbieder om te verbinden met de VoIP-server van de aanbieder. Als de aanbieder een alternatief moet bieden, dan betekent dit dat de VoIP-server van de aanbieder met een veelheid van apparaten en clients moet kunnen communiceren. De aanbieder zal waarschijnlijk ook meer alert moeten zijn op bugs, beveiliging en fraude.

Mocht de optie voor een losse SIP-verbinding gekozen worden, dan kan de aanbieder verplicht worden om de klant over te zetten van telefoonnummer naar een 085 nummer. Dit is een nummerreeks speciaal voor nomadisch gebruik. XS4All gebruikt dit nu al voor haar klanten.

Conclusie voor VoIP-diensten

Ten aanzien van VoIP-diensten is de conclusie dat het nu al voorkomt dat klanten eigen apparatuur gebruiken voor het gebruik van VoIP-diensten. Dat dit in het verleden ook voorkwam, maar dat de ondersteuning hiervan door de loop der jaren verminderd is. Mocht de verplichting komen dat klanten eigen VoIP apparatuur aansluiten, dan vergt dit vooral van de aanbieder dat deze zijn bedrijfsprocessen, security en fraudepreventie anders inricht. Er ontstaan dan meer mogelijkheden voor problemen, waar actief aandacht voor nodig is.

Overige (publieke) diensten staan los van de (vaste) netwerktoegang

Overige diensten zoals bijvoorbeeld het KPN FON open Wifi netwerk of VodafoneZiggo's Wifi-spots zijn geïntegreerd in de modem/router. In Nederland zijn dit soort diensten redelijk beperkt. In Frankrijk zijn veel meer diensten in "Le Box" zoals de Fransen het kennen geïntegreerd. Deze apparaten komen met Blu-Ray spelers, networked attached storage (NAS) waarmee klanten back-ups kunnen maken, bittorrent client, game console, photo en video programma's om opgeslagen foto's en video's op tv te tonen⁴⁸. Ze komen met apps voor mobiele telefoons, waar klanten kunnen instellingen kunnen beheren, maar ook wifi voor gasten of kinderen aan of uit kunnen zetten. In toenemende mate worden internet of things toepassingen geïntegreerd. De ontwikkeling hiervan is een continue proces met regelmatige updates en nieuwe toepassingen. Een enkele keer worden functionaliteiten ook weer afgeschakeld.

In de Nederlandse situatie zal het gedeelde wifi van VodafoneZiggo vooral een interactie met VodafoneZiggo vereisen. KPN maakt gebruik van de diensten van FON, een wereldwijd netwerk

⁴⁷ Dit is geen denkbeeldig gevaar. In de zakelijke markt is het hacken van VoIP servers en bedrijscentrales (PABX) een dagelijks gevaar.

⁴⁸ <http://www.free.fr/freebox/freebox-revolution.html>

van gedeeld wifi. Om dit op een alternatieve router werkzaam te krijgen zal een contract met Fontech nodig zijn, dat de wereldwijde dienstverlening achter dit product levert.

Het aansluiten van indoordekking mobiele netwerken is naar de mening van sommige ISPs ook een reden om de modemkeuze vrijheid te beperken. Zij stellen dat de apparatuur die gebruikt wordt om de dekking te realiseren tot hun netwerk behoort. Het betreft hier apparatuur als femto- en picocellen. Maar dergelijke apparatuur wordt door mobiele aanbieders ook gebruikt om antenne opstelpunten te ontsluiten over klantenaansluitingen op andere netwerken. De aanbieder heeft dus geen controle over de modem nodig. Ook hier is er sprake van een overeenkomst tussen eindgebruiker en aanbieder van de mobiele dienst die verder los staat van de aanbieder van de vaste netwerktoegang. Zo had Vodafone in het verleden de SignaalPlus femtocellen voor consumenten. Dit was nog voordat Vodafone vast breedband aanbod aan consumenten en deze femtocellen functioneerden op iedere breedbandaansluiting.⁴⁹

Het aansluiten van andere femtocellen dan die welke door de aanbieder aangeboden worden, wordt op dit moment niet door aanbieders toegestaan. Aanbieders beroepen zich erop dat zij deze femtocellen moeten kunnen beheeren. Er wordt een directe verbinding naar hun internet GSM/UMTS/LTE netwerk gemaakt. Daarbij geldt ook dat zij een exclusieve spectrumlicentie hebben voor de te gebruiken banden. Een eindgebruiker mag derhalve geen apparatuur aansluiten die van deze banden gebruik maakt, zonder toestemming van de aanbieder.⁵⁰

Zou er een verplichting komen om consumenten zelf femtocellen te laten toevoegen, dan zal een mobiel netwerk verplicht worden om toegang te geven tot haar netwerk. Aan de andere kant, zal het de klant ook verplichten om het mobiele netwerk toegang te geven tot de apparatuur. Dit omdat netwerken dynamisch gemanaged worden als clusters van cellen. Ook zal een mobiel netwerk zelf de mobiele telefoons die willen verbinden met haar netwerk moeten kunnen authenticeren. Consequentie zou zijn dat alleen die apparatuur welke goedgekeurd is door de mobiele aanbieder en beheerd kan worden door deze aanbieder gekocht en aangesloten kan worden. Dit lijkt niet anders dan de bestaande praktijk.

Het aansluiten van apparatuur die gebruik maakt van de DECT-guardband voor private mobiele communicatie (dus niet via de mobiele aanbieder) is nu al mogelijk en wordt bijvoorbeeld in ziekenhuizen gebruikt. Hiermee worden privé mobiele netwerken gebouwd, maar dit is buiten de scope van dit onderzoek.

Zakelijke dienstverlening

Zakelijke dienstverlening is veel minder gestandaardiseerd dan consumenten dienstverlening. In de kleinzakelijke markt wordt vaak gebruik gemaakt van een consumenten aansluiting, soms met een iets ander merkje of service niveau er op. In het midden en grootzakelijke segment bestaat een veelheid van aanbiedingen. Klanten kunnen een veelheid van modellen met en zonder eigen apparatuur krijgen. Aanbieders merken op dat voor beschikbaarheid,

⁴⁹ Zie Vodafone <https://www.vodafone.nl/support/internet-en-dekking/signaal-plus.shtml#signaalplus-instellen>

⁵⁰ Zie ook <https://www.agentschaptelecom.nl/onderwerpen/repeaters> Strikt genomen vallen repeaters buiten de reikwijdte van dit rapport omdat zij de signalen alleen op laag 1 versterken en geen rol spelen ten aanzien van modems etc. femtocellen maken wel actief onderdeel uit van het netwerk.

redundantie en prestatie het nodig is dat zij eigen apparatuur aanbieden. Vooral omdat de apparatuur beheerd wordt door de eigen organisatie en de basis legt voor de contractueel gesloten parameters.

Voor veel zakelijke aansluitingen geldt dat het belangrijkste is dat, de verbinding het doet en blijft doen. Uitval kan tot uitval van de bedrijfsvoering leiden. ISPs springen hier op in door verbindingen te leveren waar garanties op gegeven worden, bijvoorbeeld 99,9% of 99,96% van de tijd zonder verstoring (uptime-garantie). Hierbij kunnen ze ook garanties geven over wat er gebeurt bij uitval, bijvoorbeeld door redundante verbindingen aan te leggen. Ook zijn er veelal garanties over de hoeveelheid verkeer die over de lijn kan en in hoeverre daar sprake is van overboeking. De wijze waarop dit geboden wordt is veelal door een end-to-end garantie af te leveren, dus tot en met het apparaat dat bij de klant staat.

Voor de ISP geldt dat deze vertrouwen heeft in de hele keten, omdat deze de hele keten kan controleren en beheren. Als de klant zelf een eigen apparaat kan plaatsen, dan veranderen verschillende parameters, waardoor het moeilijker wordt om de klant dezelfde beschikbaarheid, redundantie en prestatie te beloven. Als er een verstoring is, dan zou deze in het apparaat van de klant kunnen zitten, de oorzaak van de verstoring in het apparaat van de klant kan weer zitten in een foutieve instelling aan de kant van de operator. Maar hoe het ook zij, er is een storing en dus wordt de uptime niet gehaald. De wijze waarop de dienst opgebouwd is en welke garantie hier aan gegeven kan worden is vooral contractueel en niet gebaseerd op de dienst zoals bedoeld in de Telecomwet. Het is goed mogelijk om een netwerkdienst te verkopen, met separaat daarvan een beheerscontract voor het eindapparaat en daar een andere garantie op te geven, dan wanneer de klant zelf apparatuur inbrengt. Hier kan ook een ander prijskaartje aan hangen.

5.3.3 Conclusies impact diensten

Voor diensten geldt dat het gebruiken van eigen apparatuur door de gebruiker voor diensten de aanbieder verplicht om:

- Duidelijke beschrijvingen te maken van de diensten
- Te specificeren welke protocollen gebruikt worden
- Te specificeren welke parameters in die protocollen gebruikt worden
- Te specificeren welke API's, software versies, chipsets etc. gebruikt of ondersteund worden
- Iedere wijziging in de eigen infrastructuur, software en protocollen te communiceren
- Iedere nieuwe dienst of functionaliteit op tijd aan te kondigen en hiervoor gedetailleerde beschrijvingen te publiceren.

Dit zal vooral operationeel voor aanbieders een wijziging betekenen voor de bestaande praktijk. Voor een dienst als VoIP zal de impact beperkt zijn, maar voor IPTV zal de impact door de huidige mate van standaardisatie veel groter zijn omdat additionele diensten volledig gespecificeerd moeten zijn.

Voor bepaalde diensten; internettoegang en telefonie, is het goed mogelijk dat consumenten hun eigen apparatuur kiezen. Dit zijn volwassen, wereldwijde markten met standaarden.

Voor diensten als kabelTV zijn er wereldwijde standaarden, maar veel additionele functionaliteit is lokaal geïmplementeerd en veel additionele functionaliteit kent korte ontwikkelcycli. De basisdienst kan veelal met een standaard apparaat afgenomen worden, maar additionele functionaliteit zal niet werken. Diensten als IPTV kennen geen jarenlange standaardisering en zijn veelal fabrikant en provider specifiek, en bovendien dwingen content providers bepaalde oplossingen en restricties af. Dit maakt het moeilijk voor telecomaanbieders deze diensten te specificeren en deze specificatie up to date te houden. Netwerkaanbieders kunnen er voor kiezen de betreffende diensten aan te bieden via apps en/of smartcards, waardoor die specificatie eenvoudiger kan zijn of deels naar standaard koppelvlakken kan worden verwezen. Met name het beschikbaar stellen van content via een app is reeds een zichtbare marktontwikkeling bij telecomaanbieders.

In de zakelijke markt is een mogelijke oplossing het werken met andere contractvormen, zodat de garanties anders gegeven worden. Geen aanbieder kan gedwongen worden tot garanderen van apparatuur die zij niet geleverd heeft. Voor bestaande en lopende contracten zou de nieuwe regelgeving wat dat betreft geen impact moeten hebben. Maar definitieve conclusies ten aanzien van juridische impact en contractimpact zijn buiten de scope van dit onderzoek.

5.4 Issues rond impact op eigen netwerk en eigen apparatuur

5.4.1 Belangrijkste effecten

Sommige internet providers richten hun netwerk al wel zo in dat zelf routers en wifi access punten plaatsen gemakkelijk is, bij anderen is dit een probleem doordat routerfunctie en AP functie op het door de operator geleverde modem niet gemakkelijk kan worden uitgezet of kan worden omzeild.

Volgens sommige reacties is de door operators meegeleverde apparatuur op dit moment juist ondermaats. Met soms bewezen onvolkomenheden (bijvoorbeeld o.a. chipset Intel PUMA). Andere reacties noemen de huidige situatie energie onzuinig en milieu onvriendelijk: de meegeleverde apparatuur is nu juist erg energie onzuinig en overstappen levert e-waste op door ongebruikte oude modems.

5.4.2 Validatie van de technologische argumenten

Waar het eigen netwerk van de gebruiker begint is het onderwerp van discussie. De aanbieders stellen zich op het standpunt dat het interne netwerk van de gebruiker begint achter de een door de aanbieder beheerde actieve component. De aanbieder beheert volgens hen het netwerk tot aan de LAN poort van het actieve apparaat. De eindgebruiker beheert het eigen netwerk tot aan de LAN poort van eigen apparatuur. De verbinding wordt gemaakt door een passieve kabel waarmee de eindgebruiker zelf de twee domeinen verbindt.

Voor het kabelnetwerk van VodafoneZiggo klopt deze beschrijving, doordat het bij Ziggo mogelijk is om een kabelmodem in bridgmodus te zetten. Zoals beschreven, levert de modem dan alleen de pakketjes door. In netwerken van andere aanbieders, zoals KPN, wordt bridge-modus lang niet altijd ondersteund. Dat betekent dat de consument ook de router, firewall, NAT en router van de aanbieder heeft te accepteren. In feite strekt daarmee het netwerk zich verder dan de definitie die de aanbieders zelf geven. In de praktijk betekent dat bij veel klanten

dat het netwerk van de aanbieder zich strekt tot en met het Wifi-netwerk van de klant. Daarmee zou het interne netwerk in het huis van de gebruiker ook tot het netwerk van de aanbieder behoren.

Als de firewall/NAT en router niet uitgezet kunnen worden, dan kan dit voor problemen in het netwerk van de klant zorgen als de klant zelf ook apparatuur plaatst. Gedacht kan bijvoorbeeld worden aan een mesh-Wifi oplossing om betere wifi dekking in huis te krijgen. Er ontstaat dan een zogenoemde dubbele NAT, hetgeen meestal niet voor problemen hoeft te zorgen, omdat ontwikkelaars er rekening mee houden, maar wel bijvoorbeeld bij online games⁵¹.

Het is echter niet te verwachten dat er problemen ontstaan in de netwerken van de aanbieders als een gebruiker zijn eigen router gebruikt en die van de aanbieder uit zet. Niet voor niets zijn er aanbieders die de klant de mogelijkheid bieden om een modem in bridge modus te zetten. Zoals in de vorige sectie al gezegd zijn er in de router geen geïntegreerde veiligheidsdiensten beschikbaar bij Nederlandse ISP's dus een gebruiker zal niet onveiliger zijn met een eigen router. Ook het netwerk van de aanbieder zal niet onveiliger worden.

5.4.3 Conclusies eigen netwerk en eigen apparatuur

Een vrije routerkeuze zal geen negatieve effecten hebben op het functioneren van het interne netwerk en het netwerk van de telecomaandbieder. Het zal consumenten wel meer mogelijkheden geven hun interne netwerk vorm te geven. Aanbieders mogen geïntegreerde oplossingen blijven aanbieden. De vrije modemkeuze zal het echter moeilijker maken om de gehele infrastructuur te controleren.

5.5 Issues met betrekking tot standaarden netwerkaansluiting

5.5.1 Belangrijkste issues

Met betrekking tot standaarden wordt enerzijds opgemerkt dat er duidelijkere aansluitstandaarden nodig zijn voor interoperabiliteit en flexibiliteit. Anderzijds wordt door de operators ingebracht dat de praktijk van standaarden weerbarstig is en ook binnen één netwerk lokaal verschillend.

Over de passieve aansluiting in de meterkast brengen de aanbieders naar voren dat de wijze waarop de Beleidsregel omgaat met de passieve aansluiting in de meterkast niet strookt met de bestaande praktijk. Zij noemen daarbij een aantal issues, met name met betrekking tot glasvezelaansluitingen:

- *Er mag geen NT (NTU) meer aangelegd worden als onderdeel van operator netwerken.*
- *Zonder NT geen overeengekomen kwaliteit.*
- *Aansluiten kan alleen door vakbekwame monteurs.*
- *Er moet voorkomen worden dat een interfacebeschrijving of standaard de keuzevrijheid juist beperkt.*

⁵¹ Ubisoft over problemen met dubbele NAT. <https://support.ubi.com/en-GB/faqs/000026724>

5.5.2 Validatie van de issues rond standaarden van de (passieve) aansluiting

Verplichte publicatie van specificaties werkt beter dan voorschrijven van technische standaarden. Maar er zijn wel aandachtspunten.

Technische standaarden evolueren snel, en omdat er verschillende typen aansluitnetwerken zijn met verschillende technologieën, elk met eigen innovaties, is het niet zinvol om expliciet technische standaarden voor te schrijven. De huidige aanpak om publicatie van specificaties voor te schrijven is daarom het meest werkbaar. Wel is het zinvol om na te denken over:

- Een eventuele *verplichte reikwijdte* van de te publiceren specificaties iets scherper te formuleren. Idealiter zou dit gaan om specificaties van alle relevante functionele lagen (vermoedelijk in ieder geval OSI laag 1, 2 en 3), dus van fysieke aansluiting tot en met welke IP variant wordt gebruikt.
- Een eventuele *verplichte minimale termijn waarop wijzigingen in de specificaties worden gepubliceerd* en waarop specificaties zullen worden ingevoerd of juist uit gefaseerd. Dit om te voorkomen dat consumenten apparatuur aanschaffen die binnen zeer korte termijn niet meer bruikbaar is.

Bij glasvezelaansluitingen mag een NT nog steeds worden aangelegd door de telecomaandbieder, maar is geen onderdeel van het operator netwerk. Een FT is dat wel.

Het argument dat geen NTU meer zou mogen worden aangelegd heeft betrekking op de koppeling van de fysieke laag en de transportlaag. In enkele gevallen is door aanbieders een signaal omzetter ingezet, welke de conversie van optisch Ethernet naar elektrisch Ethernet doet. Deze heeft een externe energiebron nodig. Voor bijvoorbeeld KPN is dit standaard, maar dit is niet de standaard bij alle aanbieders. Zo gebruiken T-Mobile Thuis, Fieber en fiber.nl geen NTU.

Het punt dat hier gemaakt wordt gaat een stap te ver. Het hebben van het demarcatiepunt voor de NTU betekent dat in theorie een klant zijn apparatuur rechtstreeks kan aansluiten op de glasvezel. Gezien het feit dat dit in de praktijk ook mogelijk is bij verschillende ISPs lijkt dit technisch niet bezwaarlijk te zijn. Echter er is geen verbod op het uitleveren van een NTU en veel gebruikers zullen hier mogelijk dan ook voor kiezen, omdat het aansluiten op een NTU veelal eenvoudiger zal zijn.

Kwaliteitsbewaking is ook mogelijk zonder NT

Dit argument ziet vooral op de transportlaag. Hiervoor zijn effectief 2 hoofdstandaarden (Ethernet en GPON) met verschillende snelheden actief in Nederland. Deze standaarden zijn in hoge mate uniform voor alle technologieproducenten. Het mag dan ook redelijkerwijs verwacht worden dat deze netwerken ook functioneren met een Ethernet of GPON aansluiting van een andere fabrikant.

Ook een consument kan – met voldoende uitleg – glasvezel koppelen aan een NT (NTU)

Het argument dat aansluiten alleen kan door vakbekwame monteurs stelt dat de fysieke aansluiting van een NTU op een glasvezel vakbekwaamheid benodigd heeft. Dit argument is moeilijk te volgen aangezien de FTU zo ontworpen is dat de gebruiker zelf de NTU of een combinatie

van NTU en modem kan aansluiten op de FTU. Fiber Nederland heeft op Youtube⁵² voor alle in gebruik zijnde FTU's een handleiding gezet, zodat de gebruiker dit zelf kan. Ook andere aanbieders, zoals bv Online kennen dit soort handleidingen.

Er moet voorkomen worden dat een interfacebeschrijving of standaard de keuzevrijheid juist beperkt

Er is altijd een kans dat partijen de mazen van de regelgeving proberen op te zoeken en specificaties publiceren die in de praktijk niet, of alleen met veel moeite en kosten, door derden zijn te gebruiken om alternatieve producten in de markt te zetten. Hoe dit te voorkomen ligt buiten de scope van dit onderzoek, een mogelijkheid is om ergens de optie tot ex-post handhaving te formuleren. Het verdient in ieder geval aanbeveling dat het ministerie of ACM regelmatig evalueert of de geest van de wet nog wel wordt nageleefd en eventueel actie te ondernemen als dit niet het geval mocht zijn.

5.5.3 Conclusie standaarden netwerkaansluiting

De huidige technologie neutrale benadering van verplichte publicatie van specificaties lijkt het meest werkbaar, maar termijnen en reikwijdte verdient aandacht.

Er lijkt weinig reden tot zorg te zijn ten aanzien van de passieve aansluiting. Deze aansluiting wordt nu al aangelegd op een manier waardoor de consument niet zelf de glasvezel hoeft te monteren. Het enige dat een consument kan doen is een kabel of NTU koppelen. Aangezien veel ISPs een zelfinstallatie programma hebben, lijkt dit niet tot onoverkomelijke problemen te lijden.

⁵² <https://www.youtube.com/playlist?list=PL1gHwW04uyIt2xOh7aDIDLnqaCQBXFQv4> en <https://www.online.nl/uploadedFiles/Content/Widgets/Content/klantenservice/extra-informatie/Genexis-P1090.pdf>

6 Analyse beheersbaarheid

In hoofdstuk 2 is een overzicht gegeven van het bredere beleidskader. In Hoofdstuk 5 worden de verschillende issues die kunnen ontstaan behandeld. De vraag ontstaat dan of een situatie waarbij gebruikers een vrije modemkeuze hebben nog wel beheersbaar is. Vanuit dat beleidskader verkent dit hoofdstuk de mogelijke opties voor mitigerende maatregelen die de veiligheidsrisico's kunnen beheersen. Hierbij wordt ingegaan op mogelijke rollen voor netwerkaanbieders, fabrikanten en eindgebruikers, en maatregelen die zij kunnen nemen, en de effecten op korte en langere termijn.

Impact Consumenten

Het is maar zeer de vraag hoe gebruikers zullen reageren op de vrije modemkeuze. Verwacht kan worden dat de marktwerking hier zijn werk zal doen. Als de aanbieders een modem/router leveren die door de gebruikers als goed genoeg beoordeeld wordt, dan zal er weinig animo zijn om een ander apparaat te gebruiken. Mocht de aanbieder echter een modem/router gebruiken die voor problemen zorgt, dan hebben gebruikers meer de neiging om over te stappen.

Uiteindelijk gaat het er de meeste gebruikers om dat alles "gewoon werkt". In het verleden kozen gebruikers voor eigen routers en wifi, wanneer zij bijvoorbeeld geen dekking boven hadden. Dit stimuleerde aanbieders weer om wifi-oplossingen te leveren welke "gewoon" met hun oplossing werkten. Nu meer en meer apparaten in huis online komen wordt er meer en meer van de modem/router van de aanbieder gevraagd. Zolang de door de operator geleverde modem/router kan leveren wat de gebruiker wil, zal de gebruiker vooral van de door de operator aangeboden standaard oplossing gebruik maken. Zodra de oplossingen van de aanbieder niet voldoen, zal de gebruiker naar een andere modem/router overstappen.

De eis dat het gewoon werkt, zal maken dat voor diensten als VoIP en IPTV de behoefte van consumenten voor eigen apparatuur beperkter zal zijn dan bij modems. De kans is namelijk groot dat de zelf aangeschafte apparatuur niet altijd volledig zal samenwerken met alle nieuwe functionaliteit van de dienstverlener. Dit creëert vanuit het perspectief van de gebruiker "gedoe". Tenzij deze apparatuur echt vernieuwende of belangrijke aanvullende⁵³ functionaliteit toevoegt zal dit in de beschreven omstandigheid niet iets zijn waar consumenten op zitten te wachten. Het mag worden verwacht dat onder invloed van de beleidsregel de mogelijkheden voor het aanbod van goed werkende alternatieve apparatuur toe zal nemen maar het is niet goed voorspelbaar of en hoe snel deze ontwikkeling zal plaatsvinden.

Impact aanbieders

In de praktijk zal de vrije modemkeuze waarschijnlijk voor weinig problemen zorgen. Ook nu laten aanbieders al een veelheid van modems toe op hun netwerken. Aanbieders moeten dus in hun operationele processen rekening houden met meerdere typen modems. Wat aanbieders zullen moeten doen is beter communiceren over modems die compatibel zijn met hun netwerk, welke instellingen hiervoor nodig zijn en of er administratief nog wijzigingen nodig zijn (bijvoorbeeld een registratie van de gebruikte modem), en in hoeverre er actieve

⁵³ Als de standaard modem alleen zeer beperkte functionaliteit heeft biedt dat ruimte voor andere aanbieders om bijv. opnamefunctionaliteit aan te bieden.

klantondersteuning wordt geboden voor bepaalde modems. Voor de consument kan dan ook duidelijk worden dat bepaalde modems minder compatibel zijn en/of in de toekomst daardoor mogelijk voor problemen kunnen zorgen. Ook zal bekend moeten zijn tot wanneer bepaalde modems en instellingen compatibel blijven, zodat consumenten ook rekening kunnen houden met vervangingscycli.

Het is echter wel de vraag of een vrije modemkeuze aanbieders zal stimuleren om te voldoen aan open standaarden. Het zou ook kunnen zijn dat bepaalde aanbieders kiezen voor standaarden die slecht ondersteund zijn en/of maar door één leverancier geleverd worden. Op deze wijze kan de klant alleen kiezen voor modems van die fabrikant. Alhoewel de regelgeving stelt dat de gegevens over de interfaces en standaarden gepubliceerd moet worden, zegt dit niets over patenten, licenties, fabrikant-specifieke oplossingen, etc. Dit kan ertoe leiden dat fabrikanten minder bereid zijn om modems te maken voor de betreffende netwerken. Wel moet hierbij gezegd worden dat een operator die kiest voor 1 specifieke oplossing van 1 leverancier in de toekomst vaak hogere kosten zal hebben, omdat zijn onderhandelingsruimte beperkter zal zijn. Vandaar dat veel operators een bewust beleid hebben voor een multi-vendor strategie.

Voor operators betekent de vrije modemkeuze wel, dat bij problemen in het netwerk alternatieve modems een rol kunnen spelen. Echter, in de praktijk ondersteunen de meeste aanbieders al een veelheid aan compatibele modems en dus valt het niet te verwachten dat dit tot een onoverkomelijke hoeveelheid problemen leidt.

Voor de ontwikkeling van nieuwe diensten kan het gebruik van eigen eindapparaten wel tot problemen leiden. Een eigen modem kan deze nieuwe dienst mogelijk niet ondersteunen. Het zou er mogelijk toe kunnen leiden dat de aanbieders gaan kiezen voor meer app-gebaseerde dienstverlening. Apps, die werken op televisie en mediabox platformen, zoals die van Samsung, LG, Apple en Android-TV. De andere kant op achten wij het minder waarschijnlijk dat fabrikanten speciale systemen zullen bouwen om volledig met het IPTV platform van 1 specifieke Nederlandse aanbieder te kunnen werken. Het is niet alleen de beperkte markt, maar ook de complexiteit van het bouwen van een systeem van hardware en software, wat misschien altijd achter de versie van de ISP aanloopt.

Impact fabrikanten

Vanuit de fabrikanten van modems en VoIP apparatuur is er een duidelijke vraag naar meer keuzevrijheid voor de eindgebruiker. Het is een markt met redelijk stabiele standaarden en afdoende lange termijn zicht op marktontwikkelingen. Zij zijn ook bereid hiervoor nieuwe apparatuur te ontwikkelen. De impact voor hen zal dan ook vooral een grotere markt zijn, waar zij meer mogelijkheden hebben om zich te onderscheiden.

Voor televisie zal het complexer zijn om in te stappen. De markt kent geen standaarden. Zelfs als een ISP gebruik maakt van open source (zoals XMBC) dan is het zeer waarschijnlijk dat dit een zeer specifieke eigen implementatie is, een zogenaamde fork. Het vergt waarschijnlijk veel nieuwe software om een andere implementatie te laten werken. Mochten ISPs met apps komen die op een veelheid van platformen werken, dan zal er wel een druk zijn op fabrikanten om hun tv's en media-apparaten te laten samenwerken met deze apps.

Rol innovators en early adopters

Voor consumenten zal de vrije modemkeuze wel “handig” kunnen zijn wanneer de gebruiker een niet-standaard oplossing wil. Vaak wordt een niet-standaard oplossing gekozen door een consument die voor de markt uit loopt. Dit was goed zichtbaar toen gezinnen een betere dekking op meerdere verdiepingen wilden hebben. Er verschenen handleidingen online en handige vrienden werden gevraagd om een extra wifi-toegangspunt toe te voegen. Op dit moment zijn Wifi-mesh en het Internet of Things voorbeelden van toepassingen waar consumenten al druk mee bezig zijn, maar waar aanbieders nog geen oplossing voor hebben.

7 Conclusie, impact en aandachtspunten

7.1 Doel

Het doel van het onderzoek was om op basis van de consultatieresultaten een inschatting van mogelijke risico's te verkrijgen in puur technische zin (wat kan er potentieel misgaan, gegeven het huidige niveau van beveiliging door fabrikanten bijvoorbeeld). Deze risico's werden vervolgens bezien in de *context* van:

- 1) mogelijke *operationele, technische en contractuele maatregelen* die *netwerkaanbieders* kunnen nemen om de desbetreffende veiligheidsrisico's te adresseren;
- 2) mogelijke *ontwikkeling ten aanzien van niveau van beveiliging van eindapparaten* door *fabrikanten*;
- 3) *verantwoordelijkheden* die bij *eindgebruikers* kunnen worden belegd voor de *beveiliging van private netwerken*.

Dit rapport heeft als uiteindelijk doel een handvat te bieden om de specifieke argumenten uit de consultatie van de beleidsregel die betrekking hebben op veiligheidsrisico's, adequaat te kunnen beoordelen en mee te nemen in een uiteindelijk besluit.

7.2 Aanpak

Het ministerie heeft Stratix gevraagd om alleen naar de praktische en technische consequenties van de vrije keuze van eindapparaten te kijken. Stratix heeft dit gedaan door te kijken naar:

1. Issues rond impact op het netwerk van de operator
2. Issues rond de impact op veiligheid
3. Issues rond de impact op diensten
4. Issues rond de impact op het eigen netwerk en de eigen apparatuur van de gebruiker
5. Issues met betrekking tot standaarden van de netwerkaansluiting

Voor ieder van deze issues is gekeken naar de belangrijkste effecten zoals genoemd door de respondenten, een validatie van deze argumenten en op basis hiervan een validatie.

7.3 Conclusie

Over het geheel kan gezegd worden dat de vrije keuze van eindapparaten weinig effecten heeft op het functioneren en de veiligheid van het netwerk. Er zijn wel effecten te verwachten ten aanzien van de organisatie en ten aanzien van het aanbieden van diensten, als VoIP en IPTV. Voor bepaalde diensten, zoals IPTV en andere multimediale diensten zijn de effecten vrij groot. Het verschil wordt veroorzaakt door de mate van standaardisatie welke plaatsgevonden heeft voor de dienst. Netwerken, VoIP, kabeltelevisie zijn allen wereldwijd gestandaardiseerd. Dit

vereenvoudigt het instappen van andere fabrikanten in de markt en het gebruik van de producten van deze fabrikanten door gebruikers.

Als een consument een DSL-, FTTH of Docsis modem koopt en deze voldoet aan de standaarden welke door de ISP gebruikt worden, dan is er weinig reden om te verwachten dat de consument of de ISP hierdoor problemen zullen ervaren. Zelfs al mocht er een productiefout in het apparaat zitten, dan zal veelal het apparaat niet uit zichzelf gaan zenden als er geen goede verbinding is. De kans op negatieve effecten op het netwerk van de ISP en/of de andere gebruikers is daarmee dan ook zeer beperkt.

De veiligheid van modems en routers is een complexe aaneenschakeling van leveranciers die allen een deel van de veiligheid bijdragen. Er is maar een beperkt aantal leveranciers van chipsets in de wereld, waardoor de consument en de ISP modems kopen die op vergelijkbare chipsets gebouwd zijn. De veiligheid van deze chipsets en de systemen die er op gebouwd zijn, zijn afhankelijk van fabrikant van de modem en de snelheid waarmee deze problemen oplost. In het geval er een probleem zit in een modem die geleverd wordt door een ISP, dan is het waarschijnlijk dat het effect groot zal zijn omdat tienduizenden gebruikers deze modems gebruiken. In het geval het een probleem is in een modem die door een eindgebruiker is aangeschaft, dan zal het effect beperkter en meer verspreid zijn. De geschiedenis heeft echter uitgewezen dat zowel fabrikanten, ISPs als gebruikers niet goed acteren bij het verhelpen van problemen. Een vrije modemkeuze verlaagt of verhoogt de veiligheid van modems en routers niet, maar zorgt er wel voor dat gebruikers een alternatief hebben.

Het is ook niet waarschijnlijk dat het netwerk van de aanbieder onveiliger zal worden door de vrije modemkeuze. De modems van de aanbieders spelen op dit moment geen essentiële rol in het beveiligen van de netwerken van de providers. Ze zijn niet beter of slechter beveiligd dan modems/routers die gekocht kunnen worden. Er zit geen andere, betere of slechtere hardware of software in en de fabrikanten zijn niet beter of slechter dan die waar consumenten toegang toe hebben.

Wel verdient de veiligheid van en door apparaten en software achter de modem/router voortdurende aandacht. Maar dit staat los van de modemdiscussie en is binnen deze discussie ook niet of nauwelijks aan te pakken. Dit gaat om veiligheidsaspecten van consumenten apparatuur en mogelijke risico's voor andere apparatuur binnen en buiten het consumentennetwerk. Deze risico's zijn slechts zeer beperkt te beperken door maatregelen op of rond het modem.

De voorgestelde wijzigingen op Europese regelgeving zullen hier waarschijnlijk een positief effect hebben op de veiligheid van de apparatuur, zoals modems. Verwacht kan worden dat de voorgestelde wijzigingen in regelgeving zullen leiden tot een verbetering van de beveiliging van eindapparatuur (waaronder modems) en een betere beveiliging van persoonsgegevens. Het lijkt er echter niet op dat, om dit doel te bereiken, de keuze van consumenten voor eindapparatuur (waaronder modems) beperkt zal worden.

De markt voor multimediale diensten en IPTV is minder goed gestandaardiseerd. Alhoewel onderdelen wel gestandaardiseerd zijn, bv de codering van een tv-signaal, is het geheel van de dienst voor iedere telecomaandbieder op een andere manier samengevoegd. Dit betekent dat een andere fabrikant (of een opensource project) zal moeten weten hoe het geheel van de dienst van de telecomaandbieder is samengevoegd. Het zal dan niet meer genoeg zijn om een aantal protocollen en instellingsparameters te noemen, maar er zal gecommuniceerd moeten

worden over API's, versies, bugs, workarounds etc. Dit verhoogt de complexiteit om de mogelijkheid om alternatieve hardware te gebruiken aan te bieden. Hierbij dient te worden aangetekend dat het construeren van die apparatuur en software in de praktijk vooral zaak zal zijn voor de fabrikant, niet voor de telecomaانبieder zelf. Maar de telecomaانبieder is wel als eerste verantwoordelijk dat alle interfaces in voldoende mate openbaar zijn. Telecomaانبieders kunnen er ook voor kiezen de betreffende diensten aan te bieden via apps en/of smart-cards, waardoor die complexiteit wordt beperkt. Met name het beschikbaar stellen van content via een app is reeds een zichtbare marktontwikkeling bij telecomaانبieders.

Voor zakelijke dienstverlening zal de vrije modemkeuze tot een andere inrichting van contracten kunnen leiden. ISPs verkopen nu diensten met garanties ten aanzien van beschikbaarheid, prestatie en redundantie. De ISP zal veelal van mening zijn dat als de klant een eigen modem gebruikt, de ISP niet gehouden kan zijn om daarvoor garanties te geven. De contracten zullen hierop aangepast moeten worden.

Ten aanzien van de eigen netwerken van de eindgebruiker geeft de vrije keuze van eindapparatuur wat meer flexibiliteit ten aanzien van de inrichting van dit netwerk. Opties als ouderlijk toezicht, mesh wifi en geavanceerdere vormen van filtering zitten niet in de modem/router combinaties van ISPs maar worden wel meer en meer gemeengoed in de consumentenmarkt.

Het zelf kunnen koppelen van apparatuur op glasvezelaansluitingen was volgens een aanbieder iets wat alleen door getrainde professionals gedaan kan worden. Voor de zakelijke markt zijn hiervoor redenen genoemd als lagere toleranties bij hogere datasnelheden en over het algemeen zeer strikte SLA's. In de consumentenmarkt is de praktijk echter divers: andere aanbieders hebben filmpjes op Youtube gezet hoe consumenten zelf de modem op de glasvezelplug kunnen aansluiten.

Mogelijke effecten op langere termijn

De vrije modemkeuze is strikt juridisch misschien niet een wijziging in het beleid van het Ministerie, maar het is wel een breuk met de bestaande praktijk van de ISPs. Deze zijn veelal in hun bedrijfsprocessen gewend geraakt aan een situatie waar zij bepalen welke apparatuur er bij consumenten staat. Soms is het in de huidige situatie al mogelijk om een ander, alternatief apparaat te gebruiken, of is er een mogelijkheid om het meegeleverde apparaat in een modus te plaatsen waarbij een deel van de functionaliteit wordt omzeild, de zogenaamde 'bridge modus'. In die gevallen waar het technisch mogelijk is om een eigen modem te gebruiken, vergt dit veelal nog wel eigen handigheid van de consument en staan niet alle benodigde gegevens en instellingen de site van de ISP. Het is niet waarschijnlijk dat netwerken door een vrije modemkeuze minder veilig worden of dat de dienstverlening aan andere klanten in gevaar komt. Een vrije modemkeuze verandert vooral de bedrijfsprocessen ten aanzien van ondersteuning van consumenten.

Een vrije keuze van apparatuur voor VoIP zal grotere effecten hebben. De veiligheid van VoIP is nu al een punt van zorg voor telecomaانبieders. Gehackte VoIP-centrales worden actief misbruikt en aanbieders proberen deze centrales op te sporen en blokkeren om de kosten van frauduleuze gesprekken van deze centrales te beperken. Een vrije keuze van VoIP apparatuur en verbindingen kan risico's op hoge kosten voor consumenten met zich meebrengen.

Een vrije keuze van Set Top Boxen (STBs) voor televisie zal complex zijn. STBs zijn slecht gestandaardiseerd. Elke ISP en fabrikant heeft een eigen variant. De ontwikkelingen gaan ook zeer snel, met ongeveer elke 6 weken een nieuwe versie. Dit betekent dat een fabrikant van een alternatieve STB elke ontwikkeling en wijziging zal moeten ontvangen om deze zelf te kunnen implementeren. Een mogelijk gevolg zou ook kunnen zijn, dat televisiediensten “over the top” worden aangeboden, los van het onderliggende netwerk. De televisiedienst wordt dan een applicatie die op apparatuur van de gebruiker kan draaien. In een dergelijk geval valt de televisiedienst niet onder de in dit rapport besproken regelgeving. In een dergelijk geval zou de consument mogelijk ook uit verschillende over-the-top televisiediensten kunnen kiezen.

Literatuurlijst

- [1] Vragen van de leden Van Toorenburg (CDA) en Verhoeven (D66) aan de Ministers van Justitie en Veiligheid en van Economische Zaken en Klimaat over het bericht «Experts: overheid moet ingrijpen bij internetapparaten» (ingezonden 17 januari 2018).
- [2] Antwoord van Minister Grapperhaus (Justitie en Veiligheid), mede namens de Staatssecretaris van Economische Zaken en Klimaat (ontvangen 7 maart 2018). Zie ook Aangangsel Handelingen, vergaderjaar 2017–2018, nr. 1097. <https://www.tweedekamer.nl/kamerstukken/kamervragen/detail?id=2018Z00494&did=2018D17812>
- [3] Staatsblad, Besluit van 12 december 2016 houdende regels inzake eindapparaten ter implementatie van richtlijn 2008/63/EG, <https://zoek.officielebekendmakingen.nl/stb-2016-524.html>
- [4] Concept beleidsregel netwerkaansluitpunt, https://www.internetconsultatie.nl/beleidsregel_netwerkaansluitpunt
- [5] Ontwerp toelichting beleidsregel netwerkaansluitpunt, https://www.internetconsultatie.nl/beleidsregel_netwerkaansluitpunt
- [6] Richtlijn 88/301/EEG van de Commissie van 16 mei 1988 betreffende de mededinging op de markten van telecommunicatie-eindapparatuur <http://eur-lex.europa.eu/legal-content/NL/TXT/HTML/?uri=CELEX:31988L0301&from=EN>
- [7] Richtlijn 2008/63/EG VAN DE COMMISSIE van 20 juni 2008 betreffende de mededinging op de markten van telecommunicatie-eindapparatuur <https://eur-lex.europa.eu/legal-content/NL/TXT/HTML/?uri=CELEX:32008L0063&from=en>

Annex A Samenvatting consultatiereacties

Deze annex bevat een samenvatting van de consultatiereacties. In deze versie zijn alleen de openbare reacties samengevat, en bijbehorende bron(nen) genoemd. Een aantal issues werd zowel in openbare als niet-openbare reacties genoemd. Daarvan zijn hier alleen de openbare bronnen vermeld. Issues die uitsluitend in niet-openbare reacties zijn vermeld zijn in deze versie niet zichtbaar.

A.1 Netwerkt toegang, operator netwerk

A.1.1 Instellen eigen modem leidt mogelijk tot slechtere prestaties of storingen

Volgens meerdere reacties zou het onwenselijk zijn dat klanten zelf hun eigen modem kunnen instellen, omdat dit kan leiden tot slechtere prestaties van de eigen verbinding of zelfs van verbindingen van andere klanten of zou kunnen leiden tot een toename van storingen. Dit is zowel een mogelijk beheersprobleem als een veiligheidsprobleem (zie ook volgende paragraaf)

Communicatie daarover met de aanbieder is moeilijk als het een eigen apparaat betreft dat anders is dan het standaard apparaat van een aanbieder. De ondersteuning van vele verschillende typen modems is moeilijker dan de ondersteuning van één of een beperkte set modems, en leidt mogelijk tot meer storingen. Ook is de verantwoordelijkheid voor een juiste instelling van het modem onduidelijk. [BIR][ZET][LAN][LEI][CAR]

In een aantal reacties wordt geopperd om in ieder geval bridging mode te verplichten als optie op standaard bijgeleverde modems "sommige huidige modems/routers zitten helemaal op slot " [LEI][FIJ]

Een reactie suggereert dat operators desgewenst betaalde extra ondersteuning kunnen aanbieden [VEN]

A.1.2 Bij Docsis 3.x en VDSL is de kwaliteit van de doorgifte van het signaal voor een gehele wijk afhankelijk van het functioneren van alle modems in die wijk.

Een afwijkend of onbekend Docsis of VDSL modem op één aansluiting kan daarbij mogelijk negatieve impact hebben op kwaliteit van andere aansluitingen [BIR]

Als niet duidelijk is van welk modem een stoorsignaal afkomstig is, is er volgens een reactie van de gezamenlijke operators soms geen andere methode dan één voor één de afgaande takken van het netwerk los te maken tot het stoorsignaal verdwijnt. [BIR]

A.1.3 Prestatiegaranties (zie ook 'regelgeving')

Prestatiegaranties zijn aan klanten met een eigen modem niet of in mindere mate te geven door een operator. Het alternatieve modem is wellicht van mindere kwaliteit, of kan een lagere capaciteit of snelheid aan of heeft minder uitgebreide features. Ook is het niet in alle gevallen mogelijk om het modem te gebruiken om de prestaties van het operator netwerk tot aan de rand van het netwerk van de klant te meten. [BIR]

A.1.4 Wholesale aanbod moeilijker (zie ook ‘regelgeving’)

Aanbieders van open glasnetwerken (zoals CAI Harderwijk, KT Waalre, Reggefiber) leveren dienstverlening op 2 lagen. Sommige aanbieders maken gebruik van NTU van glasnetwerk, met alleen eigen router, anderen plaatsen eigen NTU. In de nieuwe regels kan de aanbieder van open glasnetwerk niet meer de kwaliteit van verbinding richting wholesale klanten monitoren en garanderen [BIR]

A.1.5 SLA (zie ook ‘regelgeving’)

Art. 1.3 definitie van NTU is onwerkbaar bij een moderne IP gebaseerde elektronische communicatiedienst. NTU bij de klant is essentieel om SLA te monitoren en te handhaven. [EUR]

A.1.6 Mobiele netwerken

Ook bij mobiele netwerken is er sprake van apparatuur op locatie van de abonnee die tot het domein van de aanbieder zou moeten behoren. Operators gaan er van uit dat deze apparatuur buiten de beleidsregel valt, maar lid 4 van de beleidsregel roept hierbij vragen op. [BIR][Niet openbaar]

A.1.7 [Niet openbaar]

[Niet openbaar]

A.1.8 [Niet openbaar]

[Niet openbaar]

A.2 Veiligheid

A.2.1 Zorgen van operators over gevolgen voor veiligheid en continuïteit van beleidsregel

In een aantal reacties wordt bezorgdheid of angst verwoord dat de beleidsregel eerder negatief dan positief uitpakt voor de veiligheid van netwerken [EUR][TEL][BIR]

A.2.2 Als klant verkeerde instellingen kan gebruiken verlaagt de netwerkveiligheid

Hierbij zijn een aantal in een eerdere paragraaf genoemde argumenten en issues relevant: communicatie tussen operator en klant over instellingen is moeilijk als het een apparaat betreft waarvan een operator minder kennis heeft. Ondersteuning vele verschillende typen modems is lastig, leidt mogelijk tot meer storingen. Verantwoordelijkheid is onduidelijk. [BIR][ZET][LAN][LEI][CAR]

Andere genoemde issues en argumenten met betrekking tot veiligheid uit de consultatiereacties zijn:

- Operators dienen identificatie, authenticatie en/of beveiligingsfunctie gegevens te verstrekken aan abonnees [PAS][BID][BAR][WVR]
- Certificering van losse modems / routers etc. is nodig [BOO]

- Onderhoud van modems die niet door de provider ter beschikking worden gesteld kan geen verplichting zijn voor een operator. Dit geeft risico's op het gebied van internet-veiligheid. [BIR]
- [Niet openbaar] DOCSIS firmware updates mogen nu alleen door operators worden uitgevoerd. Dit moet worden aangepast (beter dan in Duitsland) [MUN]

A.2.3 Veiligheid vanuit verschillende perspectieven

[Niet openbaar]

De beveiligingsfunctie moet volgens enkele reacties niet verward worden met de toegangsfunctie, en kan best anders worden uitgevoerd dan hoe het door operators nu gebeurt. [PEE][JOO]

Een consultatiereactie stelt dat veel consumenten veiligheids-issues niet snappen, en dat het daarom beter is de firewall bij de operator te laten [FIJ]

Een andere reactie vreest: de consument dreigt veiligheidsexpert te moeten worden [SCH]

A.2.4 Uitzondering Identificatie Authenticatie Beveiligingsfunctie

Artikel 1.5 is bruikbaar omdat het een uitzondering creëert voor apparaten met een bij het netwerk behorende identificatie- authenticatie- of beveiligingsfunctie. Het onderscheid tussen hardwarematige en softwarematige componenten is gekunsteld: hardwarematige functies kunnen in veel gevallen ook softwarematig worden uitgevoerd. [TEL]

SIM-kaarten toestaan leidt mogelijk tot de introductie van SIM achtige apparaten die uiteindelijk de vrije modemkeuze weer teniet doen [QUA][MAA]

A.3 Diensten

A.3.1 TV set top boxen

TV set top boxen vallen (mogelijk) onder de beleidsregel. Het doorgeven van auteursrechtelijk beschermde content noodzaakt gebruik van bepaalde hardware. Reikwijdte is nu onduidelijk [BIR]

[Niet openbaar]

[Niet openbaar]

DRM in eindapparaten is onwenselijk: consument maakt al legitiem gebruik van de aangeschafte producten [VRI]

A.3.2 Andere diensten zoals telefonie en wifi hotspots

Ten aanzien van de diensten telefonie en wifi hotspots zijn de consultatiereacties nogal divers.

[Niet openbaar]

Sommige reacties van operators spreken van Wifi hotspot diensten als aparte dienst (die alleen over de meegeleverde box geleverd kan worden). Andere operators die ook een dergelijke dienst aanbieden noemen alleen dat de gebruiker zelf kan beslissen of hij de door de operator meegeleverde Wifi functionaliteit wil gebruiken.

A.4 Eigen netwerk en apparatuur

A.4.1 Over de flexibiliteit van de huidige situatie wordt zeer verschillend gedacht

[Niet openbaar]

[Niet openbaar]

Meegeleverde apparatuur nu juist ondermaats. Met soms bewezen onvolkomenheden (voorbeeld o.a. chipset Intel PUMA). [BOE][WEB]

Huidige situatie is energie onzuinig en milieu onvriendelijk: Meegeleverde apparatuur nu juist erg energie onzuinig en overstappen levert e-waste op door ongebruikte oude modems [BOE][JOO]

A.4.2 Verantwoordelijkheden scheiden

Verantwoordelijkheden voor apparatuur dient duidelijk te zijn (operator vs. Eindgebruiker/fabrikant) [HAG]

De scheiding tussen draadloze modems, bedrade modems, routers, andere apparaten zoals TV ontvangers, is volgens sommige reacties niet duidelijk genoeg [VRI]

A.5 Definities en consistentie van regelgeving

A.5.1 [Niet openbaar]

[Niet openbaar]

[Niet openbaar]

A.5.2 Achterliggend probleem onduidelijk

Aan de geconsulteerde beleidsregel ligt geen kenbaar onderzoek ten grondslag naar de wenselijkheid en gevolgen voor zowel klanten, aanbieders als apparatuur leveranciers, en geen kosten/baten analyse. Procedure is weinig zorgvuldig. [BIR][TEL].

Oplossing voor niet bestaand probleem [EUR]

Zal geen effect hebben op de markt van eindapparaten [BIR]

A.5.3 Het is geen verduidelijking, maar een wijziging

Het gaat niet om een verduidelijking, maar om een wijziging van het wettelijk kader [BIR] Het besluit eindapparaten suggereert dat operators geen apparatuur mogen afsluiten. De toelichting zegt dat dit eventueel wel mag. Maar een toelichting heft de verwarring niet op. [BIR]

A.5.4 Timing

Een aantal reacties vinden de timing onduidelijk. Redelijke implementatietermijn is vereist. Voorstel loopt mogelijk uit pas met Europa [BIR][EUR]

A.5.5 Mogelijke strijdigheid met overige regelgeving

Een aantal reacties claimen dat het voorstel strijdig is met overige regelgeving, zoals het Informeren van minimale, normaliter beschikbare en maximale internetsnelheden (Europese verordening Netneutraliteit 2015/2120, richtsnoeren BEREC en beleidsregel ACM) gaat over snelheden 'op het modem'. Bij eigen modemkeuze kan geen adequate informatie worden verstrekt. [BIR][TEL]

Voorstel is strijdig met regeling over compensatie bij storingen [TEL]

[Niet openbaar]

[Niet openbaar]

A.5.6 Formulering regelgeving is onduidelijk

art. 1.1. Definitie 'openbaar' is onduidelijk en kan mogelijk misbruikt worden [MAA]

art. 1.2. Definitie is onhelder en mogelijk valt PoP apparatuur hier ook per ongeluk in [MAA]

art. 1.3. Het verbinden van de definitie met wel of niet elektriciteit bieden biedt mogelijk een loophole [MAA]

Art. 1.5 is onduidelijk: wat valt er wel en niet onder? Kan het niet misbruikt worden door operators waardoor vrije modemkeuze alsnog niet mogelijk is? Vallen TV decoders hier onder? [LUG][DAV][COU][MAA][PEE]

A.6 Standaarden netwerkaansluiting

A.6.1 Aansluitstandaarden nodig voor interoperabiliteit en flexibiliteit

Aansluitstandaarden nodig voor IP(v4/v6) en diensten als telefonie, TV, radio [STE]. Blijkbaar zijn sommige reactieschrijvers van mening dat duidelijker, eenduidiger en meer technisch gerichte aansluitstandaarden hier beter werken dan de in de regelgeving gekozen algemene en techniek neutrale formulering.

A.6.2 Standaarden soms niet interoperabel / uniform

De praktijk ten aanzien van technische standaarden is weerbarstig. Standaard compliant apparatuur is niet altijd interoperabel. Standaarden zijn - ook bij dezelfde operator - niet overal in het land hetzelfde [BIR]

A.6.3 Standaarden veranderen: informatieplicht nodig

Informatieplicht over termijn uitfasering standaarden is nodig, om te voorkomen dat consument apparaten aanschaft die na een paar maanden niet meer nodig zijn of moeten worden hergeconfigureerd [BID]

A.6.4 Interfacebeschrijving of standaard moet niet juist keuzevrijheid beperken

De interfacebeschrijving of standaard moet niet zodanig zijn dat aanbieders hun apparaten, diensten en/of netwerken zo kunnen ontwerpen dat zij een beroep op een uitzondering kunnen doen of geen keuzevrijheid aan hun abonnees hoeven te bieden [VTK].

A.7 Overige opvallende reacties

A.7.1 Ontevredenheid met huidige situatie

Huidige situatie biedt kosten en privacy-schendingen aan voor functionaliteit die de gebruiker niet per se wil, zoals Wifi [DER][KAA]

[Niet openbaar]

A.7.2 Supporters voor de gedachte achter de beleidsregel

Helpt om functionaliteit van routers bereikbaar en bruikbaar te maken voor gebruikers met kennis [MUL][QUA][JOO][VTK]

Bevordert concurrentie door betere scheiding publiek/privé netwerk. Niet alleen in prijs maar ook in kwaliteit. Overstappen wordt gemakkelijker voor consumenten en MKB. [WEB][JOO][VTK]

[Niet openbaar]

A.7.3 Kritiek op de gedachte achter de beleidsregel

Aanschaf aansluiting + modem wordt duurder op deze manier, bij standaardapparaten maar zeker als gebruiker iets anders wil hebben LAN][VRI]

Aanschaf aansluiting + modem of router wordt ingewikkelder op deze manier, ook voor bijv. ouderen [JUM]

[Niet openbaar]

[Niet openbaar]

[Niet openbaar]

Annex B Overzicht openbare reacties

Nr	Code	Naam	Organisatie	Plaats	Korte inhoud	Bijlage
1	TEL	H Heinink	Tele2	Diemen	onderscheid hard- en software in art.1.5 is gekunsteld. Let op veiligheid, kosten/baten, consistentie andere regelgeving	ja
3	BIR	MC Minne- cré-Kracht	div. Telecompro- viders	Den Haag	Analyse onvoldoende, diverse veiligheids-/continuïteitsbezwaren, DRM issues	ja
4	EUR	R van Kes- sel	Eurofiber	Maarssen	Demarcatiepunt beleidsregel niet werkbaar. Zorgen veiligheid en conti- nuïteit. Timing inwerkingtreding niet te begrijpen.	ja
6	VTK	NJ Linssen	VTKE	Nijmegen	Verheugd met beleidsregel. Aansluitpunt is gaandeweg verkeerd geïnterpreteerd door aanbieders. Slecht voor verkoop.	ja
9	JOO	PM Joosten		Amsterdam	Vrije keuze is goed. O.a. mogelijkheden voor HTPC. Energie-, milieube- sparing. Operators kunnen anders beveiligen dan nu.	ja
10	MUN	D Munk		Groningen	Beleidsregel verwoordt beleid nu beter. Firmware updates beter regelen dan in Duitsland, met operator verplichting	ja
12	PEE	HZ Peek		Amsterdam	1.5 beveiligingsfunctie hoort niet in een apparaat voor toegang, maar via secure identificatie of authenticatie	
15	MAA	MG Maat- huis		Eindhoven	1.1 definitie openbaar onduidelijk, 1.2 formulering onduidelijk, 1.3 mo- gelijk complicaties 1.5 zwakbodem	
18	QUA	ERG Quaeghe- beur		Amsterdam	Operator modems hebben artificiële beperkingen (voor TV). SIMkaarten toestaan leidt mogelijk tot geen vrije keuze.	

Nr	Code	Naam	Organisatie	Plaats	Korte inhoud	Bijlage
19	WVR	W de Vries		Joure	Groot voorstander van deze regel. Voordeel weegt op tegen nadeel voor operator dat ze gegevens moeten vrijgeven.	
21	SCH	THM Schoemaker		Utrecht	Met betrekking tot mededinging: toelaten is één ding, ondersteunen is iets anders. Security dreigt slachtoffer te worden.	
22	FIJ	H de Fijter		Roosendaal	Veiligheid is zwaarwegend issue. Gemiddelde consument snapt dit niet. Firewall bij operators. Wel in bridge mode.	
23	STG	P ter Steege		Amsterdam	Beter en sneller modem wordt mogelijk, nadeel is dat ondersteuning provider achterblijft bij ontwikkelingen	
24	VEN	JG van de Ven		Sint Oedenrode	Beleidsregel geeft gewenste keuzevrijheid. Eventueel kunnen operators extra betaalde ondersteuning aanbieden	
26	KA	GV Kaal		Apeldoorn	Doen! Ik wil absoluut geen wifi.	
27	CAR	AIR Caris		Fluitenberg	Dit gaat grote problemen geven. Ondersteuning andere modems is onmogelijk. Levert kastje muur gedrag op.	
32	HAG	M Hagoort		Groningen	Blij met regel. Verantwoordelijkheid apparatuur moet wel duidelijk zijn (operator vs eindgebruiker/fabrikant)	
33	BAR	V Barnar		Houten	Operators (KPN) leveren stelselmatig geen informatie over instellingen van eigen modem. Hopelijk verbetert dit.	
35	LEI	HS Leisink		Delft	Keuzevrijheid betekent ook ondersteuning van alle modems door providers. Betere optie is bridging mode eisen.	

Nr	Code	Naam	Organisatie	Plaats	Korte inhoud	Bijlage
36	JUM	J Jumelet		Leerdam	Voor ouderen wordt dit allemaal moeilijker en ingewikkelder	
37	DER	CF Derksen		Lent	Onacceptabel dat apparaat van internetleverancier toegang heeft tot privé netwerk: privacy, kosten	
39	VRI	J Vries		Den Haag	Benoem verschillen tussen draadloos/bedraad/routers/tv ontvangers. Bezorgd dat het netto duurder wordt.	ja
40	BID	S Biddle		Amsterdam	Maak expliciet dat diensten functionaliteiten beschikbaar blijven op andere apparaten. Denk aan uitfasering.	
42	LAN	W Lankman		Hattem	Eigen modem/router kan nu al. Ondersteuning is mogelijk probleem. Maatregel kost geld.	
45	WEB	PDF Weber		Enschede	Fantastisch initiatief. TV ontvangers bij providers kwalitatief onder de maat. Dit bevordert vrije markt.	
46	COU	H Couvée		Leeuwarden	Ander modem echt mogelijk? Ziet uitzonderingen waardoor 'monopoly' mogelijk niet wordt aangepakt.	
48	PAS	ZJ Pasop		Zeegse	Nieuw geheim password Telfort maakt gebruik Fritzbox/AVM modem onmogelijk.	
49	BOE	LH van Boeijen		Amsterdam	Nogal blij met deze regel. Hulde aan deze nieuwe regel. Meegeleverde hardware inferieur.	
50	ZET	W. Zettlinger		Roosendaal	Vreest - als monteur - verlaging zekerheid netwerk. Operators zijn best bekend met 'eigen' hardware	

Nr	Code	Naam	Organisatie	Plaats	Korte inhoud	Bijlage
51	DAV	H Davids		Arnhem	Erg voor. Art. 1.5 verdient extra aandacht. Operators moeten zich hier niet achter kunnen verschuilen	
52	LUG	JD Lugtenburg		Apeldoorn	Art. 1.5 is onduidelijk: wat valt er wel en wat niet onder?	
58	BOO	WJ Bootsma		Houten	Extra losse modems en losse routers moeten mogelijk blijven. Certificering kan oplossing zijn.	
60	STE	SJM Steffann		Apeldoorn	Aansluitstandaarden nodig voor IP(v4) en diensten zoals TV, telefonie en radio	
63	MUL	Erik Mulder		Driebergen	Goed initiatief, Telecomproviders zetten routers dicht. Als ICT'er wil ik zelf kunnen kiezen	

Annex C Overzicht niet openbare reacties

[Niet openbaar]

Annex D Overzicht achtergrondinformatie

Deze annex bevat een tabel met een overzicht van aanvullende achtergrondinformatie die is gebruikt bij het opstellen van dit rapport. Deel van deze achtergrondinformatie is niet openbaar. De betreffende velden zijn aangegeven met [Niet openbaar].

Nr	Bron	Titel	Datum	Open- baar	Short Summary	Observations
1	[Niet openbaar]	[Niet openbaar]	[Niet open- baar]	nee	[Niet openbaar]	[Niet openbaar]
2	Franz Jürgen Säcker, Multi-media und Recht 2015 (translated)	The Freedom of Choice of Terminal Equipment in Telecommunications: A Plea against the ISP lock	2015	ja	This paper introduces the draft bill for the selection and connection of terminal equipment in telecommunications, through which the practice by several network operators of prescribing certain terminal equipment to their end customers – known as the "ISP lock" – is to be eliminated. Once the Federal Network Agency was no longer able to protect the right of choice for users of terminal telecommunications devices, it became legally relevant and in the interest of competition policy for the German federal government not to wait years for judicial clarification, but rather to act itself in keeping with the coalition agreement and submit an amendment to the TCL that produces freedom of competition on the market for telecommunications terminal devices. It is to be hoped that the clear, precisely formulated draft bill will pass parliamentary obstacles as soon as possible	

Nr	Bron	Titel	Datum	Open- baar	Short Summary	Observations
3	[Niet openbaar]	[Niet openbaar]	[Niet open- baar]	nee	[Niet openbaar]	[Niet openbaar]

4	Excentis, commissioned by ANGA (ANGA Verband Deutscher Kabelnetzbetreiber e.V., https://www.anga.de/)	Study on the Network Termination Point of Internet access and Telephony over Cable Networks (HFC)	jan 29, 2015	ja	This document is the result of a study by Excentis on the Network Termination Point (NTP) for Internet Access and Telephony over cable networks (Hybrid Fibre Coax infrastructure (HFC)). It is concluded that the NTP in cable networks should be the well-known and consumer familiar Ethernet interface. - As the most important criterion this view puts the responsibility regarding the proper operation of the delivered service (esp. the internet speed) on the cable operator. --This is because only in this case the cable operator remains fully responsible (and in control) of the complex interaction between cable modem (CM) and cable modem termination system (CMTS). --The customer on the other hand still has full flexibility to connect any device (router, computer, etc.) to the Ethernet interface on the cable modem.	no TV in title? Interesting overviews of HFC related arguments from the perspective of HFC operators
---	---	---	--------------	----	---	---

					The analysis also shows that the Radio Frequency (RF)-interface should not be defined as the NTP. This is due to many reasons: - In a cable network there is the possibility that one bad modem interferes with the inter-net and telephony service of a large group of customers. - Allowing customers to use or install their own software on cable modems is a very big security risk to cable networks and has to remain impossible at all means, since it can introduce problems both related to network operations (interfering with the services of many other users), and as well problems related to security and authentication. - Modems might have specific interoperability issues with the network and/or equipment of the operator. A Cable Modem purchased by the consumer might not be compatible with the network or become incompatible during the network's evolution. Such equipment would have to be replaced by the consumer. - Retail Modems might not be ready for new services that the operator wants to offer. - Consumers have no easy way to check the speed offered at the RF-interface; on the other hand, the speed offered to the CMCI interface can easily be verified.	
--	--	--	--	--	--	--

Nr	Bron	Titel	Datum	Open- baar	Short Summary	Observations
5	[Niet openbaar]	[Niet openbaar]	[Niet open- baar]	nee	[Niet openbaar]	[Niet openbaar]

6	[Niet openbaar]	[Niet openbaar]	[Niet openbaar]	nee	[Niet openbaar]	[Niet openbaar]
---	-----------------	-----------------	-----------------	-----	-----------------	-----------------

Nr	Bron	Titel	Datum	Open- baar	Short Summary	Observations
7	[Niet openbaar]	[Niet openbaar]	[Niet open- baar]	nee	[Niet openbaar]	[Niet openbaar]
8	[Niet openbaar]	[Niet openbaar]	[Niet open- baar]	nee	[Niet openbaar]	[Niet openbaar]
9	c't 2013, Heft 14	Providers Freud	2013	ja	Een goede introductie over hoe het in Duitsland begon. Feitelijk zei BNetzA dat zij niets doen voor consumenten. C't legt uit dat deze argumentatie wel zeer moeilijk te begrijpen is gezien de wetteksten en de richtlijnen. Daarbij blijken Duitse ISPs allerlei rotzooi getrapd te hebben waardoor klanten extra, verborgen kosten voor hun routers betalen moesten (wifi-activatie fee) en Carrier Grade NAT in kabelnetwerken.	Waard om een klein stukje extra aandacht aan te geven. Duitse ISPs lieten alle slechte kanten zien.

Nr	Bron	Titel	Datum	Openbaar	Short Summary	Observations
10	Unitymedia	Position Statement of Unitymedia KabelBW concerning the Draft Bill on Choice and Connection of Telecommunications Terminal Equipment	2015	ja	De Engelse variant lijkt gelijk te zijn aan de Duitse variant. Unitymedia is van mening dat zij geen passief interconnectiepunt biedt en dat daarom de wet fout is. Ze doen heel gewichtig over grondwet etc. Waar het verhaal interessanter wordt is dat ze zeggen dat hun netwerk onveilig wordt, omdat het een shared medium is. Volgens UnityMedia zou dit schending van de privacy van eindgebruikers zijn als hun burens toegang hebben tot het signaal.	
11	[Niet openbaar]	[Niet openbaar]	[Niet openbaar]	nee	[Niet openbaar]	[Niet openbaar]
12	[Niet openbaar]	[Niet openbaar]	[Niet openbaar]	nee	[Niet openbaar]	[Niet openbaar]
13	[Niet openbaar]	[Niet openbaar]	[Niet openbaar]	nee	[Niet openbaar]	[Niet openbaar]
14	EZ	Telekommunikationsgesetz (TKG)	dec-16	ja	De Duitse Telecomwet	

Nr	Bron	Titel	Datum	Open- baar	Short Summary	Observations
15	EZ	Law on the selection and connection of terminal equipment in telecommunications	29-1-2016	ja	vertaling van 15?	
16	[Niet openbaar]	[Niet openbaar]	[Niet open- baar]	nee	[Niet openbaar]	[Niet openbaar]

Annex E Interviews n.a.v. het conceptrapport in het kader hoor-wederhoor

E.1 Inleiding

E.1.1 Achtergrond en overzicht

De door het Ministerie van Economische Zaken en Klimaat (EZK) voorgenomen beleidsregel 'vrije modemkeuze' is in december 2017 – februari 2018 geconsulteerd door middel van internetconsultatie. Er zijn in die periode diverse consultatiereacties binnengekomen, waarvan de reacties van de operators en van de verkopers van apparatuur het meest uitgebreid zijn.

EZK vroeg aan Stratix ondersteuning om techniek gerelateerde argumenten over gevolgen van vrije modemkeuze die in het kader van de consultatie mogelijk op tafel komen, goed te kunnen adresseren. Stratix concludeerde in een draft rapportage dat de vrije keuze van eindapparatuur voor wat betreft modems en voip-telefoons beperkt effect zal hebben op het technisch functioneren van netwerken. De veiligheid van gebruikers blijft gegarandeerd. Er zullen wel procedurele en organisatorische wijzingen bij aanbieders nodig zijn. Een vrije keuze van set-top boxen voor televisie kan wel ingrijpende technische problemen met zich mee brengen. De argumenten en kanttekeningen zijn omvangrijker en mogelijk verstrekkender dan verwacht werd voorafgaand aan het onderzoek. Gegeven deze resultaten van het onderzoek vond EZK het wenselijk om een traject van "hoor- en wederhoor" toe te passen met betrekking tot een geselecteerd aantal marktpartijen die op de consultatie hebben gereageerd.

Stratix benaderde daarom in opdracht van EZK een aantal partijen om individuele gesprekken over de technisch inhoudelijke argumentatie in de rapportage te voeren. De selectie is gemaakt op basis van marktaandeel en de technisch inhoudelijke reactie op de consultatie. De geïnterviewde partijen zijn (in alfabetische volgorde): CAIW en NLConnect, Eurofiber, KPN, Tele2, T-Mobile, VodafoneZiggo en VTKE (Verbund der Telekommunikations-Endgerätehersteller).

In het gesprek kregen de organisaties de gelegenheid om op de concept uitkomsten van het onderzoek te reageren door middel van een interview. Hiervoor werd het concept rapport onder embargo ongeveer twee weken voorafgaand aan het gesprek met de partijen gedeeld. Van elk interview is een gespreksverslag gemaakt dat ter review is voorgelegd aan de betreffende interviewpartij. De reacties daarop zijn vervolgens door Stratix verwerkt om tot een definitief openbaar gespreksverslag te komen, dat vervolgens geaccordeerd is door de betreffende interviewpartij.

In paragraaf E.1.2. zijn beknopt de algemene observaties samengevat

In paragraaf E.1.3. is een overzicht gegeven van wijzigingen die in het concept rapport zijn uitgevoerd na de interviews.

De gespreksverslagen zijn toegevoegd aan deze annex in de volgende paragrafen:

- E.2. Interviewverslag CAIW en NLConnect
- E.3. Interviewverslag Eurofiber
- E.4. Interviewverslag KPN

- E.5. Interviewverslag Tele2
 - o E.5.a. bijlage bij gespreksverslag Tele2
- E.6. Interviewverslag T-Mobile
- E.7. Interviewverslag VodafoneZiggo
 - o E.7.a. bijlage bij gespreksverslag VodafoneZiggo
- E.8. Interviewverslag VTKE, Verbund der Telekommunikations-Endgerätehersteller

E.1.2 Algemene observaties

Algemene observaties van issues en observaties naar aanleiding van het conceptrapport die door meerdere partijen worden genoemd:

- Meerdere partijen vinden het jammer dat het rapport zich voornamelijk beperkt tot technische argumenten en dat de organisatorische aspecten maar ten dele en de juridische aspecten niet worden meegenomen in het rapport.
- Meerdere partijen stellen vraagtekens bij de gevolgde procedure rond het aankondigen van de beleidsregel.
- Meerdere partijen noemen de wenselijkheid om het demarcatiepunt op een andere plek te definiëren, bijvoorbeeld na de modem op Ethernet/UTP kabelniveau.
- Meerdere partijen vinden dat het rapport onterecht positief is ten aanzien van de technische oplossingen van de problemen. Met name omdat de bijbehorende kosten niet duidelijk zijn.
- Meerdere partijen vinden dat het rapport in de argumentaties te veel gebruik maakt van algemene verwachtingen en aannames. Hier is tegen in te brengen dat de algemene verwachtingen en aannames gedaan zijn door Stratix op basis van kennis en expertise van markt en technologie, en dat ten tijde van het schrijven van dit rapport weinig publieke en onderbouwde informatie beschikbaar was, en ook dat in de consultatiereacties vaak alleen algemene verwachtingen en aannames gebruikt zijn en dat verder onderzoek helaas buiten de scope van dit project valt.
- Meerdere partijen vinden dat het rapport een aantal issues ten aanzien van set top boxen wel beschrijft, maar dat dit vervolgens niet voldoende in de conclusies wordt meegenomen.
- Meerdere partijen noemen het ontbreken van een beschouwing over zakelijke diensten, en het verschil tussen consumentendiensten en zakelijke dienstverlening en de implicaties hiervan.
- Meerdere partijen vinden een zorgpunt dat de regelgeving eenzelfde dienst mogelijk moet maken met een meegeleverde en een zelfgekozen eindapparaat. Met name bij zakelijke diensten is een SLA een belangrijk deel van de dienst. Deze is met een zelfgekozen eindapparaat vaak moeilijk of niet te garanderen door de dienstaanbieder.
- Meerdere partijen gaven aan dat het gebruik van definities beter kan. Zo wordt in het rapport op een aantal plaatsen over modems gesproken waar juist andere of bredere functionaliteit wordt bedoeld.
- Een aantal partijen gaf aan dat er nog een splitsing van functies NTU en FTU zou kunnen worden toegevoegd in het plaatje in de inleiding.
- Een aantal partijen vreest dat de implicaties van de beleidsregel niet stroken met bestaande verplichtingen rond het publiceren van de haalbare internetsnelheden op adressen.

E.1.3 Wijzigingen in draft rapport naar aanleiding van de interviews

Naar aanleiding van de interviews zijn een beperkt aantal wijzigingen en toevoegingen aangebracht in het draft rapport. Naast het oplossen van enkele kleine omissies is hier en daar de tekst verhelderd of zijn observaties en conclusies waar nodig aangescherpt. Hierbij zijn de suggesties uit de interviews zo goed mogelijk ter harte genomen, maar uiteindelijk eigen keuzes gemaakt: technologie, jargon en belangen van de geïnterviewde partijen lopen soms sterk uiteen en onze uitdaging was een leesbaar rapport met algemene observaties te maken waarbij tegelijkertijd de diversiteit van de consultatiereacties zo goed mogelijk recht wordt gedaan.

In de interviewverslagen wordt bij een aantal observaties verwezen naar betreffende paragrafen, en soms worden delen van het conceptrapport geciteerd. Het is mogelijk dat de betreffende paragrafen en citaten inmiddels zijn aangepast en/of opnieuw genummerd.

Hieronder volgt een beknopte opsomming van de wijzigingen in het finale rapport ten opzicht van het conceptrapport:

<u>Paragraaf</u>	<u>Wijziging ten opzichte van het in de interviews besproken conceptrapport</u>
1. Inleiding	
1.2 Doel van het onderzoek	Afbakening van de scope verder toegelicht.
1.3 Methodiek	Interviewronde toegevoegd in omschrijving en verwijzing naar deze annex.
3. Technische achtergrond	
3.2 Horizontale netwerk analyse: indeling naar netwerktopologie	Diagram aangepast en uitgebreid. Tekst aangepast, o.a. de rol van de NTU iets beter toegelicht.
4. Inventarisatie en groepering issues	
4.7. Standaarden netwerk-aansluiting	Ingevoegd in de consultatie genoemd issue rond mogelijke strategisch productontwerp.

Paragraaf

Wijziging ten opzichte van het in de interviews besproken conceptrapport

5. Analyse: Validatie technische argumenten

5.1 Issues rond impact op Operator Netwerk

5.1.2 Validatie van de technische argumenten

Bij kopernetwerken opmerking toegevoegd over ADSL DSLAMs.

Bij glasvezelnetwerken opmerking over PON toegevoegd. Verschil genoemd tussen zakelijke en consumentenmarkt bij glasvezelaansluiting.

5.3 Issues rond impact op diensten

5.3.1 Belangrijkste effecten

Opmerking toegevoegd over impact zakelijke markt.

5.3.2 Validatie van de technologische argumenten

Tekst en subconclusie met betrekking tot set top boxen verduidelijkt.

5.3.3 Conclusies impact diensten

Conclusies uitgebreid met tekst over zakelijke toepassingen en tekst over TV en set top boxen verbeterd.

5.5 Issues met betrekking tot standaarden netwerkaansluiting

5.5.2 Validatie van de issues rond standaarden van de (passieve) aansluiting

Korte analyse strategisch productontwerp toegevoegd.

7. Conclusie, impact en aandachtspunten

7.3 Conclusie

Zakelijke aspecten benoemd in conclusie. Conclusie uitgebreid met beschouwing termijn effecten.

Bovenstaande wijzigingen betreft wijzigingen van één of meer zinnen of aanpassingen van illustraties. Daarnaast zijn nog enkele kleine layout- en tekstuele verbeteringen op zins- of woordniveau doorgevoerd ten opzichte van de concept versie. Ook is het gebruik van terminologie op een aantal plaatsen verbeterd.

E.2 Interviewverslag CAIW en NLConnect

Interview n.a.v. conceptrapport "Beleidsonderzoek modemkeuze - Analyse consultatiereacties betreffende technische implicaties vrije modemkeuze"

Tijdstip: woensdag 12 september 2018, 10:00h.

Locatie: NLconnect, Den Haag

Aanwezig: Mathieu Andriessen, directeur van NLconnect, namens de leden van NLconnect, waaronder ongeveer 20 kleinere ISP's, maar ook fabrikanten van netwerkcomponenten,

Gerlas van den Hoven, voorzitter van NLconnect, tevens directeur Genexis. Genexis heeft als fabrikant van modems en andere apparatuur veel ervaring ook in het buitenland, zoals Duitsland.

Hans van der Giessen, regulatory affairs CAIW Diensten B.V. CAIW en DELTA/Zeelandnet hebben dezelfde eigenaar; beide bedrijven zijn bij NLconnect aangesloten.

NLconnect en CAIW hebben samen met andere partijen via Bird & Bird een reactie op de consultatie ingediend.

Rudolf van der Berg, senior consultant, Stratix,

Sietse van der Gaast, senior consultant, Stratix.

E.2.1 Algemene indruk draft rapport

De algemene indruk van het draft rapport van de geïnterviewden is dat het een redelijk overzicht biedt van de in de gezamenlijke consultatiereactie genoemde technische problemen. Hun eerste indruk is dat Stratix weliswaar voor heel veel technische problemen een oplossing ziet, maar niet aangeeft in hoeverre deze proportioneel zijn of wat de juridische implicaties zijn.

De geïnterviewden vinden het jammer dat de juridische argumenten uit de consultatiereactie niet meegenomen zijn in dit draft rapport. Naar hun mening zit dat weliswaar niet in de opdracht van EZK aan Stratix maar is er een verwevenheid tussen de juridische en technische (en administratieve) aspecten als het erover gaat waar de grens tussen de domeinen van de aanbieder en de eindgebruiker wordt getrokken. In ieder geval zou volgens geïnterviewden helderder in het rapport kunnen staan welke opdracht Stratix heeft gekregen.

CAIW is een toegangs- en dienstenaanbieder op de consumentenmarkt via coax en FttH en levert ook wholesale toegang via FttH. Vanuit het perspectief van CAIW werd onder meer opgemerkt:

- Het voorstel van EZ betekent dat er meer geadministreerd moet worden, vanwege juridische of voorwaardelijke implicaties in het geval klanten in plaats van de door CAIW in bruikleen verstrekte modems en set-top boxen eigen apparatuur wensen te gebruiken. Het gaat hierbij dan om regels en beleid rond:
 - o compensatie bij storingen
 - o bedrijfscontinuïteit

- beveiliging
 - opgave internetsnelheden
- Het publiceren van specificaties of verwijzen naar standaarden is niet in alle gevallen eenvoudig mogelijk. Sommige toepassingen zijn op maat gemaakt en bij andere (telefonie en interactieve televisie) moet bij de formulering van de specificaties goed rekening gehouden worden met de mogelijkheden van misbruik en fraude.

Vanuit het perspectief van NLconnect werd in aanvulling opgemerkt:

- We zien een heel duidelijk verschil tussen de netwerklaag en de dienstenlaag. Ook binnen FttH zijn vele standaarden, met als belangrijkste onderscheid punt-punt met een unieke vezel tussen PoP en klant, en PON, waarbij meerdere klanten via eenzelfde zich passief vertakkende vezel zijn aangesloten. Maar ook daarin is weer veel variatie: EPON XPON XGS PON NGPON2 zijn zo maar wat voorbeelden van verschillende PON-standaarden. Daarbij komt nog dat elke fabrikant zijn eigen smaak lijkt te hebben, die vaak niet of niet goed interoperabel zijn. Sommige bouwen voort op anderen, andere werken elkaar volledig tegen. Daarbij kent PON ook specifieke problemen. Bij PON kunnen bijv. 63 mensen op een splitter geen verbinding krijgen als één verkeerd apparaat, zoals een traditionele Ethernet aansluiting, daar licht op sproeit.
- In Duitsland worden de NTs veel meer apart beschouwd van andere apparaten zoals routers. In de praktijk is Ethernet als demarcatiepunt de oplossing; de knip leggen waar EZ hem wil gaat niet werken. Vooral in de FttH en specifiek FttH PON netwerken is er veel verschil in NTs waardoor publicatie van specificaties heel verschillend zal zijn terwijl voor de consument een glasvezel een glasvezel is. PON heeft ook meer varianten en snellere evoluties die proprietary zijn. De kans dat je zomaar een bij een (web)winkel gekocht glasvezelmodem aansluit en het werkt dan is klein, je moet heel goed weten welke variant je aansluit.

E.2.2 Specifieke punten

In het gesprek komen verschillende issues, problemen en stellingen aan de orde:

1. AVG en vrije modemkeuze
2. Piraterij van TV streams
3. Risico van malafide modemfabrikanten
4. Problemen bij glasmodems ingewikkelder door vele varianten
5. Waarom de knip niet voorbij NTU of fysieke modem?
6. SIP telefonie en IP TV zijn meest problematisch bij invoering beleidsregel

Hieronder zijn de gesprekken rond deze issues beknopt samengevat.

E.2.2.1 AVG en vrije modemkeuze

Het rapport stelt dat de AVG weinig relevantie heeft voor vrije modemkeuze (paragraaf 2.5). Volgens de geïnterviewden wekt dit de indruk dat privacy en beveiliging geen belangrijke rol spelen. Publicatie van specificaties maakt volgens de geïnterviewden misbruik en fraude eenvoudiger. Het gebruik van niet door de aanbieder gecertificeerde apparatuur vergroot volgens hen ook de kans op misbruik en fraude, bijvoorbeeld doordat er in de apparatuur 'malware' zit ingebakken. Stratix geeft als kanttekening: dan zou de encryptie hoe dan ook slecht geïmplementeerd zijn.

E.2.2.2 Piraterij TV streams

Misbruik van TV-streams (bijv. ten behoeve van piraterij) zou volgens de geïnterviewden eenvoudiger kunnen worden. Er zijn volgens hen genoeg voorbeelden van gehackte set-top boxen die het kijken van televisie zonder te betalen mogelijk maken. Bij CAIW kan de klant via interactieve televisie bestellingen doen en daar speelt bij publicatie van specificaties naar mening van de geïnterviewden weer de mogelijkheid van fraude en misbruik.

E.2.2.3 Risico van malafide modemfabrikanten

Invoer in Nederland van de beleidsregel zou er volgens de geïnterviewden zelfs toe kunnen leiden dat modemfabrikanten of resellers modems gaan verkopen inclusief malware. In Duitsland is dit niet aan de orde, de knip ligt daar in praktijk niet bij het glas. Maar "je wilt niet dat er bijvoorbeeld modems op de markt komen waarmee je 'gratis' kunt internetten".

Hoe hoger je als operator in de functionele lagen kan zitten hoe beter het volgens de geïnterviewden te beveiligen is.

Ook nu worden (bijvoorbeeld bij CAIW) door sommige gebruikers andere (coax)modems gebruikt dan de door de operator meegeleverde modems. Dit wordt wel geregistreerd vanwege bijv. uitval, garanties, teruggave etc. Maar men denkt dat het zonder certificering door de operator aantrekkelijker wordt voor criminelen om daar iets mee te doen.

E.2.2.4 Problemen bij glasmodems ingewikkelder door vele varianten

In paragraaf 5.5.2. van het concept rapport wordt beweerd dat een NTU best wel door consumenten kan worden aangesloten en dat aanbieders daar zelf Youtube filmpjes over publiceren. Volgens de geïnterviewden varieert het echter heel erg per aanbieder en gebruikte technologie of het werkbaar is om een NTU door consumenten aan te laten sluiten. Bij CAIW is zelf aansluiten mogelijk. Niet altijd is kwaliteitsbewaking mogelijk bij zelf aansluiten van vezels. Ook kan het nu misschien bij sommige technologieën werkbaar zijn omdat negatieve effecten door bijvoorbeeld vuile of verkeerd aangesloten vezels bij de nu geboden snelheden niet zo opvallen, maar als er in de toekomst hogere snelheden nodig zijn wordt een correcte aansluiting van de fysieke fiber steeds belangrijker.

- Bij punt-punt verbindingen zijn de problemen op dit moment het kleinst omdat er nog maar 1Gbit/s geleverd wordt, maar voor 10Gbit/s zijn de eisen veel strenger. Op een gegeven moment zal het ook problematischer worden dat de consument zelf wil aansluiten.
- Bij PON systemen is een stofje etc. veel eerder problematisch, ook vanwege de lagere power levels die bij dergelijke systemen gebruikt worden.

PON is wereldwijd een veelgebruikte technologie. Er komt in Nederland mogelijk meer PON aan, onder andere in het buitengebied. PON heeft voordelen (afstand), punt-punt heeft ook voordelen op andere plekken en situaties. Er zijn ook providers die dual uitrollen (PON/Punt-punt), of waarbij hybride systemen of evoluties toegepast worden.

E.2.2.5 Waarom de knip niet voorbij de NTU?

Beleidsregel 2017 maakt een knip bij de "veelgebruikte basisapparaten met een breed markt-aanbod". Geïnterviewden hebben begrip daarvoor, maar het maakt de positie van de NTU wel

onduidelijk. In paragraaf 3.2. van het draft rapport wordt de NTU/FTU beschreven. Stratix beaamt dat deze twee beter gescheiden kunnen worden weergegeven.

Mede gezien de problematiek die geschetst is in het vorige punt pleiten de geïnterviewden voor een knip tussen operator netwerk en thuisnetwerk op een net iets ander plaats: juist een knip voorbij de medium specifieke aansluiting helpt de consument, met behoud van flexibiliteit voor de aanbieder en de consument. Er zijn op dat koppelvak bij CAIW aansluitingen voor internet (inclusief een eigen al dan niet draadloze router van de consument), lineaire en interactieve televisie en telefonie.

Ook bij een eventueel streven naar standaard modemkastjes voor koper, coax en glas wordt de innovatie geremd, aldus de geïnterviewden, omdat je moet wachten totdat de standaard goed gedefinieerd en gepubliceerd is en te snelle verandering van standaarden dan niet meer gewenst is.

De grote gemeenschappelijke deler is Ethernet over koper, betoogt NLconnect: Ethernet is zeer goed gespecificeerd, goedkoop en stabiel. Men ziet Ethernet daarom als een veel beter koppelvak waar de consument echt wat aan heeft. Ook dan zijn er problemen, maar dat zijn er in elk geval veel minder dan bij het nu voorgestelde theoretische koppelvak.

E.2.2.6 SIP telefonie en IPTV zijn echt problematisch

Hier is volgens de geïnterviewden de mogelijkheid van fraude en misbruik het grootst. Bijv. fraude met betaalnummers of met het bestellen van films en andere programma's.

Op paragraaf 5.3.2 van het draft rapport wordt reverse engineering van de set top box besproken. De geïnterviewden wijzen er op dat de conclusie met betrekking tot set top boxen ontbreekt of in ieder geval veel te mager is. Er staat geen apart kopje set top boxen. Stratix ziet dat er inderdaad iets ontbreekt en zal aanpassing hiervan sterk in overweging nemen.

Daarbij komt, merken de geïnterviewden op, dat de IPTV aanpak heel verschillend is per aanbieder, en dat content providers hier ook een belangrijke rol in spelen: content aanbieders hebben rechten en stellen allerlei eisen.

E.3 Interviewverslag Eurofiber

Interview n.a.v. conceptrapport "Beleidsonderzoek modemkeuze - Analyse consultatiereacties betreffende technische implicaties vrije modemkeuze"

Tijdstip: vrijdag 7 september 2018, 14:00h.

Locatie: Eurofiber Maarssen

Aanwezig: Bart van der Snoek, product manager UNET,

Jeroen Verheijen, commercial product manager Eurofiber Nederland (actieve diensten, rand commercie),

Roel van Kessel, Manager Regulatory & Public Affairs, Eurofiber,

Hessel Idzenga, Manager Design and Architecture at Eurofiber (houdt zich bezig met actieve apparatuur 'alles waar een stekker aanzit' inclusief CPE),

Rudolf van der Berg (senior consultant, Stratix),

Sietse van der Gaast (senior consultant, Stratix)

E.3.1 Algemene indruk draft rapport

Eurofiber vindt dat de onderzoeksvraag van EZK niet helemaal duidelijk is in het rapport. Het was volgens Eurofiber logischer geweest als er een discussie was gevoerd over het demarcatiepunt en dat het rapport de verschillende opties voor demarcatiepunten met hun voor- en nadelen had beschreven. Stratix geeft aan dat de beleidsregel en de interpretatie daarvan voorvan EZK leidend was, en daarmee dus ook de bijbehorende positie van het demarcatiepunt, en dat het rapport de verschillende consultatiereacties probeert samen te vatten en – vooral in technisch opzicht – te duiden ten opzichte van dit gegeven.

Volgens Eurofiber heeft de beleidsregel een te simplistische afbakening: als er een stekker insteekt is het een eindapparaat. Eurofiber pleit ervoor dat de opdracht van EZK helderder in het rapport staat waarbij ook de interpretatie van het demarcatiepunt 'crystal clear' is.

Nederland loopt met deze regelgeving volgens Eurofiber 'voor de muziek uit': in plaats van wachten op BEREC die als gevolg van de EECC opdracht heeft gekregen om naar het demarcatiepunt te kijken. Dit leidt volgens Eurofiber op het voeren van een eigen koers die waarschijnlijk zal afwijken van de pan-Europese conclusie die BEREC gaat trekken. Daarbij leidt de voorgenomen regelgeving volgens Eurofiber op dit moment tot belemmering van innovatie in de zakelijke markt. Het gevolg zou kunnen zijn dat Nederland het beste jongetje van de klas wil zijn, maar dat andere landen niet volgen. In het beste geval zou dit volgens Eurofiber de wet van de remmende voorsprong voor de BV Nederland betekenen.

Eurofiber ziet in de discussie over deze problematiek, inclusief beleidsregel, consultatiereacties en draft rapport, een te grote nadruk op de consumentenmarkt. Als B2B aanbieder die voornamelijk gericht is op de zakelijke markt biedt Eurofiber andere diensten aan dan die in de consumentenmarkt gebruikelijk zijn, met over het algemeen veel striktere Service Level Agreements (SLA's), Eurofiber ziet niet precies welke diensten precies wel en niet onder de regel zouden moeten vallen, want veel door Eurofiber geleverde diensten zijn technisch geen

internet toegangsdienst. Vaak wordt aan klanten een verbinding geleverd inclusief een apparaat bij de klant, waarbij ook een beheercontract met Service Level Agreement voor dat apparaat zit. Hierbij komen dan vaak nog diensten als VoIP. Het kan naar mening van Eurofiber niet zo zijn dat het beheer van de apparatuur onder een internetdienst valt en dat klanten kunnen eisen dat apparatuur die zij zelf kopen beheerd moeten worden met dezelfde SLA. Die dienst is immers reeds beschikbaar bij Eurofiber, maar dan wel met een SLA die past bij een dienst waarvan Eurofiber de controle (deels) kwijt is omdat de abonnee zijn eigen CPE wil gebruiken.

E.3.2 Specifieke punten

In het gesprek werden verschillende zorgpunten genoemd, sommige naar aanleiding van het rapport, sommige meer algemeen, en soms werd tijdens de discussie teruggerepen naar eerdere zorgpunten om andere punten te verduidelijken. Dit gespreksverslag probeert een en ander beknopt en gegroepeerd weer te geven. Globaal werden de volgende punten besproken:

1. Service Levels bepaalde diensten alleen te handhaven inclusief CPE. Dezelfde dienst is ook beschikbaar zonder CPE, met de daarbij behorende (mindere) SLA
2. Flexibiliteit aanbieder binnen contract wordt ingeperkt
3. Woordgebruik en definities 'modem'
4. Leveren Managed IP VPN op CPE van derden gaat tegen ISO normering in
5. Impact op laag 3 diensten
7. Het draft rapport focust ontbrekend op consumentenmarkt. De zakelijke markt is minstens zo belangrijk.
8. Waarom niet wachten op de opdracht aan BEREC om een suggestie te doen voor een werkbaar demarcatiepunt?
9. Proportionaliteit is ver te zoeken. Kosten te eenzijdig bij aanbieders.

Hieronder zijn per punt de issues kort samengevat.

E.3.2.1 Service Levels bepaalde diensten alleen te handhaven inclusief CPE

Eurofiber stelt dat gegarandeerde service levels en een helder gespecificeerd demarcatiepunt en verantwoordelijkheden zijn bij zakelijke contracten enorm belangrijk zijn.

Eurofiber levert zowel producten zonder CPE als met CPE. Dus in die zin biedt Eurofiber de flexibiliteit al die door de nieuwe wetgeving wordt nagestreefd. Echter bij de diensten met CPE is het mogelijk hogere Service Level Agreements aan te bieden dan met de vergelijkbare diensten waarbij de klant zelf een CPE aanlevert. Bij een Eurofiber CPE kan (alleen) Eurofiber in de CPE kijken wat status en prestaties zijn, of alles aan klantkant het doet etc.

Als Eurofiber een CPE meeleverd wordt er een aanbod gedaan waarbij de fysieke laag losgekoppeld is. Als een klant zelf eigen CPEs wil gebruiken heeft dat bijv. ook impact op aantal benodigde glasvezels op het eindpunt. Bij een door Eurofiber meegeleverd CPE is het gemakkelijker om meerdere diensten te leveren over dezelfde glasvezel, meerdere VLANs bijvoorbeeld. Bij de dienst zonder CPE zal er in de Eurofiber aanpak voor elke individuele door of via Eurofiber geleverde dienst een aparte vezel geleverd moeten worden. Dit kan door Eurofiber wel geleverd worden als de klant dat wenst, maar dat is dus minder efficiënt.

Hetzelfde product leveren met de CPE keuze van de abonnee is volgens Eurofiber eenvoudigweg niet mogelijk: het product zal altijd anders zijn. Als de wetgeving verplicht alle producten gelijkwaardig aan te bieden (bij meegeleverde of eigen CPE) dan betekent dat volgens Eurofiber in feite dat de producten met een hoger Service Level Niveau niet meer mogelijk zijn, en zullen moeten worden verlaagd naar lagere gegarandeerde serviceniveaus.

Dit heeft een enorme impact op lopende en nieuwe contracten en contractvormen. De consequenties van het recht op vrije modemkeuze zijn voor Eurofiber daarom erg slecht te overzien. Als een klant gebruik maakt van iets dat in de wet staat, mogen dan wel ineens de afspraken (of een deel daarvan) tussen Eurofiber en de klant teniet verklaard worden?

E.3.2.2 Flexibiliteit aanbieder binnen contract wordt ingeperkt

Een onderdeel van een deel van de aangeboden diensten is Managed NTU (UNET Terminologie). Hierbij staan soms zelfs 2 apparaten bij klant. Het 2e apparaat wordt dan gebruikt om de netwerkconnectiviteit 'in de lucht te houden' (redundantie).

Het komt volgens Eurofiber ook regelmatig voor dat de bij de dienst behorende CPE apparatuur wordt vervangen of aangepast (natuurlijk voor rekening van de aanbieder omdat dit binnen de dienst valt). Bijvoorbeeld als apparatuur end of life is, of als nieuwe technologieën worden geïntroduceerd. Onder de nieuwe regelgeving heeft Eurofiber dergelijke flexibiliteit niet meer.

Zo is het op deze manier voor een klant ook niet van belang als er bijv. een volledig redundante of flat tail redundante of een enkele aansluiting wordt gebruikt op het laatste stukje om de gewenste (of nieuw gewenste) zekerheid te bieden.

E.3.2.3 Woordgebruik en definities 'modem'

Het woord Modem is op veel plaatsen in het draft rapport naar mening van Eurofiber niet handig gekozen en op sommige plaatsen ook niet correct. Het woord 'modem' zou volgens Eurofiber alleen op de signaalomzetting ('modulatie/demodulatie') moeten slaan (bijv. optisch naar ethernet of andersom), terwijl nu op meerdere plaatsen het woord ook gebruikt wordt voor het beschrijven van apparaten met veel meer functies dan alleen signaalomzetting. Eurofiber is bang dat een issue rond vrije routerkeuze wordt geherformuleerd naar een issue rond vrije modemkeuze terwijl dit een heel ander issue is met mogelijk een hele andere relevantie en ook hele andere mogelijke oplossingen.

Stratix geeft aan zich bewust te zijn van het belang van goede definities en het onderscheiden van verschillende functionaliteiten. In een inleidend hoofdstuk van het draft rapport worden de verschillende functionaliteiten uiteengeerafeld van het apparaat dat nu vaak met de term 'modem' wordt aangeduid. Toch is hier en daar in het draft rapport de term 'modem' blijven staan waar dit strikt genomen niet de correcte benaming zou zijn. Eén van de oorzaken hiervan is dat ook in vele consultatiereacties deze term niet consequent gebruikt is. Ook verschillen de aanduidingen van apparaten soms per aanbieder. Maar wellicht zou zeker in de latere hoofdstukken het gebruik van de term 'modem' nog eens kritisch bekeken kunnen worden.

E.3.2.4 Leveren Managed IP VPN op CPE van derden gaat tegen ISO normering in

Sommige diensten zoals die nu door Eurofiber geleverd worden en die door de markt gevraagd worden zijn volgens Eurofiber alleen mogelijk doordat apparatuur bij de klant geplaatst wordt die niet van de klant is, en waar de klant ook geen toegang toe heeft. Eurofiber geeft als

voorbeeld een Managed IP VPN dienst. Deze is volgens Eurofiber niet te leveren zonder Eurofiber router, want een andere oplossing zou ingaan de benodigde ISO normering.

E.3.2.5 Impact op laag 3 diensten

Bij sommige door Eurofiber geleverde diensten is een door Eurofiber geheel gecontroleerde laag 3 device noodzakelijk, bijvoorbeeld voor IP assignments, VoIP etc. Dit soort diensten zullen bij invoering van de beleidsregel moeten worden omgebouwd

E.3.2.6 Het draft rapport focust onterecht op consumentenmarkt. De zakelijke markt is minstens zo belangrijk.

Het draft rapport focust met name op consumentenmarkt terwijl volgens Eurofiber zowel in hoeveelheid geld als in organisatorische impact de zakelijke markt minstens zo groot is. Zelfs als in de zakelijke markt maar volgens Eurofiber weinig klanten van de mogelijkheid gebruik willen maken van de wettelijke vrijheid moeten nog steeds wel alle procedures hieraan aangepast worden.

Het is volgens Eurofiber jammer dat EZK geen onderscheid maakt tussen de best-effort consumentenmarkt en een zakelijke dienst met een hoogwaardige service level agreement waarbij het omwisselen van een CPE door een andere CPE volgens Eurofiber echt niet kan.

Eurofiber vreest dat allerlei diensten onder de regeling zouden komen te vallen waarvan dat de vraag is of dat de oorspronkelijke bedoeling is: dus niet alleen verbindingen ten behoeve van internet toegang maar ook bijvoorbeeld de eigen verbindingen die vroeger vielen onder de term 'leased lines'. De term 'openbare communicatie dienst' is immers erg breed. Bedrijven zijn een totale andere tak van sport als consumenten en de voorgenomen beleidsregel en interpretatie lijken hier volgens Eurofiber onterecht en te gemakkelijk aan voorbij te gaan.

Als voorbeeld van een te eenzijdig op de consumentenmarkt gerichte redenering noemt Eurofiber nog het stuk over zelf aansluiten van passieve apparatuur op paragraaf 7.3 pagina 57. Het zelf aansluiten van fibers zonder de juiste professionele procedures m.b.t. fibers lassen, schoonmaken van fiber uiteinden etc. is in de zakelijke markt echt niet gewenst vanwege mogelijk kwaliteitsverlies en niet kunnen nakomen van minimale kwaliteitseisen.

Stratix geeft aan dat verreweg de meeste consultatiereacties gingen over de consumentenmarkt en dat dit ook zijn weerslag heeft op de focus van het rapport. Maar het in het rapport meer expliciet noemen van de zakelijke markt is wel iets dat in overweging zal worden genomen.

E.3.2.7 Waarom niet wachten op de opdracht aan BEREC om een suggestie te doen voor een werkbaar demarcatiepunt?

Hoewel de opdracht van de EC aan BEREC in het draft rapport wel is genoemd, vindt Eurofiber het jammer dat dit aspect weinig aandacht krijgt. Eurofiber vraagt zich af waarom overheden in Europa (en EZK in het bijzonder) niet wachten op de uitkomst van het onderzoek door BEREC om een betere suggestie te doen voor een werkbaar demarcatiepunt.

Het achterliggende probleem is volgens Eurofiber voornamelijk de noodzaak tot routerkeuze en vrije keuze van andere apparatuur. Vrije modemkeuze is een totaal ander issue (zie ook 3 "woordgebruik modem") en heeft hier mogelijk veel minder mee te maken.

E.3.2.8 Proportionaliteit is ver te zoeken. Kosten te eenzijdig bij aanbieders.

De voorgenomen beleidsregel maar ook het draft rapport legt in de ogen van Eurofiber te eenzijdig de kosten voor uitvoering van de regeling bij de ISPs (zoals organisatorische aanpassingen, aanpassingen in backoffice, etc.). Eurofiber vraagt zich af: EZK is er toch niet alleen voor de consument? De proportionaliteit is volgens Eurofiber ver te zoeken. Eurofiber pleit voor onderzoek naar de economische impact van deze regeling ook ten aanzien van de impact voor de zakelijke markt.

E.4 Interviewverslag KPN

Interview nav conceptrapport "Beleidsonderzoek modemkeuze - Analyse consultatiereacties betreffende technische implicaties vrije modemkeuze"

Tijdstip: donderdag 9 augustus 2018, 10:00 h.
Locatie: KPN, Maanplein, Den Haag
Aanwezig: Lieuwe Faber, informatie analist, product manager vast/mobile, KPN
Guido Luiten, Director Fixed and Mobile Products Consumer Market (excl. TV), KPN
Paul Knol, regulatory affairs, KPN
Rudolf van der Berg, senior consultant, Stratix
Sietse van der Gaast, senior consultant, Stratix

E.4.1 Algemene indruk draft rapport

KPN geeft aan dat de discussie rond dit onderwerp een lange achtergrond heeft. In september 2016 stelde EZ in het OPT-overleg dat verduidelijkt zou worden dat het passieve aansluitpunt het demarcatiepunt is, iets wat daarvoor nog nooit zo gesteld was door EZ.

Later volgde een concept-beleidsregel en een consultatie waarop KPN reageerde, met ruwweg de volgende onderdelen (die staan samengevat op pagina 4 van de (niet openbare) KPN-reactie):

1. Bezwaren van beleidsmatige aard, en bezwaren ten aanzien van de grote impact op de bedrijfsvoering. Er is geen voorafgaand onderzoek gedaan.
2. De vraag waarom de demarcatie op een passief aansluitpunt? En niet bijv. een actieve component als laatste grens van het operator netwerk? Dit met name met het oog op de impact voor TV en Telefonie diensten
3. Ontbreken van een analyse van de timing en impact van de benodigde organisatorische transitie. EZ heeft op geen navraag gedaan naar doorlooptijden en impact.

KPN heeft geen grote onvolkomenheden of onjuistheden in het rapport gevonden. KPN vindt het jammer dat het rapport zich beperkt tot de technische vragen en opmerkingen en dat er niet meer gekeken is naar de bedrijfsmatige effecten. Het beantwoordt bijvoorbeeld niet de vraag: Wat is een redelijke tijd om markt tijd te geven om van de 'ist' situatie naar de 'soll' situatie te komen. Hiervoor zijn aanpassingen nodig aan o.a. klantprocessen, helpdesk, etc. Ook moeten wellicht zakelijke contracten opgebroken worden, etc.

Volgens KPN zou het expliciet duidelijk moeten worden gemaakt dat dit buiten de scope van het rapport valt (en dat het rapport dus niet een organisatorische impact analyse geeft), of anders zou dit veel beter naar voren moeten komen in het rapport. EZ krijgt dus naar mening van KPN met betrekking tot de organisatorische aspecten in het Stratix rapport geen input en zal voordat een implementatietermijn kan worden vastgesteld dat nog zelf moeten onderzoeken.

E.4.2 Specifieke punten

KPN noemt in het interview 4 onderwerpen waarop ze graag nog wat verder inzoomt.

1. Actief / passief, onduidelijkheid over functionele elementen en koppelvlak(ken)
2. Diensten: 1 koppelvlak, 3 diensten. EZ gooit het op één hoop, Stratix scheidt ze meer. KPN stelt dat ze zich voor telefonie aan de wet houdt door een gestandaardiseerd "telefoonaansluitpunt" te leveren. Deze mag ook op een kastje zitten, zoals een modem. Hierdoor kunnen alle standaard telefoontoestellen nog steeds worden aangesloten.
3. Specifieke impact van de beoogde beleidsregel op TV diensten.
4. Technologieën: over verschillende aspecten bij verschillende technologieën. KPN heeft ze allemaal tegelijkertijd in het netwerk. Locaties zijn verschillend, gaat niet alleen over laatste technologie maar er zijn ook nog oude technologieën die nog steeds in het veld staan, en die gefaseerd zullen worden overgezet naar nieuwere varianten.

In de paragrafen hieronder worden de discussies per onderwerp kort beschreven.

Daarnaast was er een opmerking over de beschreven beleidsachtergrond. De nieuwe Europese Elektronische Communicatie Code is nu politiek akkoord in Brussel. Dit stond (nog) niet in het draft rapport

E.4.2.1 Actief / passief

Voor KPN is het zaak om precies te weten wat er in de beleidsregel staat of komt te staan en hoe dit moet worden uitgelegd. Stratix volgt zo goed mogelijk de interpretatie van EZ en heeft geprobeerd de functionele elementen in algemene zin te beschrijven. Volgens KPN is figuur 1 onduidelijk. De term NTU staat op een verkeerde plek. Volgens KPN is een NTU mediaconverter die KPN inzet functioneel niet gelijk aan FTU, maar is deze te vergelijken met het modem zoals in figuur 1 met de modulatie/demodulatie functionaliteit. KPN wijst hierbij ook op de eigen diagrammen in haar consultatiereactie(s). Stratix zal dit proberen wat duidelijker te maken, maar wijst er wel op de uitdaging om een algemeen niet al te ingewikkeld plaatje te maken van een wereld waarbij vele implementaties en ook vele verschillende jargons gebruikt worden door aanbieders.

Ook de beschrijving van de term 'bridge mode' en het mogelijke belang daarvan voor dit rapport werd kort besproken. Bridge mode (apparaat doet alleen modem conversie en biedt geen laag 3 functionaliteit) is beschreven en besproken in het draft rapport omdat deze term in verschillende reacties is genoemd als huidige work-around of alternatieve oplossing die gebruik van eigen apparatuur door consumenten zou kunnen vergemakkelijken. Bij de uiteindelijke door EZ beoogde interpretatie van de beleidsregel is dit echter waarschijnlijk minder relevant want in feite out of scope met betrekking tot het demarcatiepunt.

KPN benadrukt ook nog maar eens dat er Europese regelgeving is ten aanzien van het halen van performance eisen, en het publiceren van de daadwerkelijk te behalen snelheden (Net-neutraliteitsverordening). Zij zien niet hoe een passief demarcatiepunt past in de boogde Europese meetmethode van BEREC.

Voorkeur van KPN is een standaard ethernet koppeling (als demarcatiepunt).

E.4.2.2 Diensten bellen/tv/internet

De telefoniedienst heeft bij KPN een lange geschiedenis. Het is bij de overgang naar nieuwe technologieën zoals VoIP steeds belangrijk geweest dat klanten een zo soepel mogelijke migratie hebben en er bij voorkeur niets of zo weinig mogelijk verandert in het telefonie thuisnetwerk. Dus alle oude telefoons met bestaande stekkertjes werken nog steeds.

De 'VoIP tunnel' vanaf de KPN box het netwerk in is daarbij met opzet afgeschermd en er worden intern authenticatie mechanismen gebruikt tussen box en netwerk om zeker te stellen dat telefoontjes echt vanaf dat specifieke thuisnetwerk plaatsvinden. Zo worden o.a. 'bill shocks' voorkomen. Bij een open specificatie van de (SIP) demarcatie kan er gemakkelijker misbruik plaatsvinden (o.a. van authenticatie gegevens) waarbij een derde persoon kan doen alsof hij via het thuisnetwerk belt. Het afschermen van het authenticatiemechanisme en de keuze om VOIP afgesloten te maken en te laten termineren de Experiabox heeft hier voornamelijk mee te maken. KPN heeft er grote voorkeur voor om de klant een kastje te geven, zelfs als de klant een eigen modem of router gebruikt. Of dit een Experiabox is of een ander kastje is om het even.

Een andere consequentie van invoer van de regel zou kunnen zijn dat je voor een klein percentage gebruikers dat niet de KPN eigen modem/router wil hebben een heel bouwwerk moet opzetten van specificaties en helpdesk instructie etc. Ook hierbij is timing ook weer belangrijk. Hoeveel tijd krijgt KPN hiervoor?

E.4.2.3 Specifieke impact van de beoogde beleidsregel op TV diensten

In Duitsland lijkt de daar geldende regelgeving met betrekking tot vrije modemkeuze helemaal geen impact te hebben op de TV set top boxen. Of is men er zich niet van bewust, want nergens blijkt dat ook set top boxen van derden (moeten) worden ondersteund. KPN kent geen voorbeelden waarin dit wel gebeurt.

De impact van het wel onder de regel laten vallen van deze apparatuur is groot volgens KPN. Dit wordt in het draft rapport al enigszins beschreven maar wat nog wat meer aandacht zou kunnen krijgen is dat met name houders van content eisen dat hun content veilig is. Zij willen hier ook controle over uitoefenen en hebben dit op diverse manieren ook geïmplementeerd. Content owners hebben onder andere een stem in op welke devices de content uiteindelijk kan worden afgespeeld. Dit maakt het vrijgeven van de keuze van devices dus moeilijker. KPN betoogt: als KPN al technische specificaties zou kunnen publiceren wil dat helemaal niet zeggen dat klanten dan ook TV diensten kunnen kijken, omdat ultimo niet KPN maar de content eigenaren beslissen welke DRM zij willen toestaan en deze content-eigenaren helemaal niet aan de Beleidsregel zijn gebonden. Dit is het probleem met de insteek van EZK, die via de definitie van netwerkaansluitpunt ook diensten wil reguleren, maar daarvoor helemaal geen wettelijke basis heeft.

In bijlage 5 van de (niet openbare) KPN reactie wordt één en ander beschreven. Partijen als Verimatrix en Movielabs behartigen hierbij de belangen van de content owners. Pas als zij een set-top box goedkeuren, kan deze gebruikt worden voor content waar gebruik gemaakt wordt van Digital Rights Management. De fabrikant/ISP heeft ook processen waarbij de eigenaren van content de toestemming kunnen intrekken.

KPN verwacht dat ISPs op termijn de eigen box uit faseren en over zullen stappen naar open platforms/apps. Het is een trend dat zaken steeds meer over the top en in apps geregeld

worden. Maar ook hier is het weer belangrijk om een realistische tijdlijn en deadlines helder te krijgen. Tijdlijnen en deadlines worden volgens KPN niet ineens realistischer doordat een aansluitpunt wordt gedefinieerd, maar zijn vooral afhankelijk van marktontwikkelingen.

E.4.2.4 Technologieën

Geen uniform netwerk, maar continue evolutie

In de praktijk is het netwerk van KPN (zoals waarschijnlijk ook van andere aanbieders) niet uniform wat betreft de gebruikte technologie. Naar de klant toe wordt wel zo veel mogelijk een eenduidige dienst geboden, ongeacht de onderliggende technologie. Bij het implementeren van de beoogde beleidsregel is een werkbare fasering voor KPN dus van het grootste belang. In het jaarverslag Netneutraliteit staat bijvoorbeeld dat de invoering mogelijk voor eind 2018 beoogd wordt. Er staat in de regelgeving en het onderzoek naar aanleiding van de consultatiereacties niets over een redelijke implementatietermijn en dat is bijzonder grote uitdaging.

VULA situatie nog niet standaard

In het rapport wordt genoemd dat (V)DSL DSLAMs tegenwoordig allemaal beheerd worden door KPN in VULA (Virtual Unbundled Local Access) oplossingen, daar waar vroeger aanbieders eigen DSLAMs plaatsten. Dit is volgens KPN niet juist. Er zijn nog heel veel locaties waar VULA oplossingen nog niet zijn geïmplementeerd. KPN moet daarom altijd nog uitgaan van de situatie dat andere partijen nog wel hun eigen spullen leveren op DSLAM niveau. KPN wijst er op dat de verplichtingen die ACM heeft opgelegd (en opnieuw wil opleggen in het geconsulteerde WFA besluit) dat ook met zich meebrengen Timing en een realistische overgangssituatie zijn daarom ook hier weer belangrijk. Dit verandert op zich niets aan de conclusies ten aanzien van het gebruik van verschillende modems op het netwerk van KPN. Alternatieve aanbieders gebruiken toch al eigen modems en KPN heeft bij Nokia capaciteit beschikbaar, waar andere aanbieders hun nieuwe modems kunnen testen.

Storing modem op andere lijnen

Ten aanzien van de beschouwing rond vectoring/ ruisonderdrukking van (V)DSL maakt KPN nog de volgende opmerking: In principe wordt alleen de 'storende' modem terugschakeld, maar voordat dat gebeurt kan het zijn dat de rest van de straat toch nog even kort last van de storende modem heeft. Volgens KPN is overigens het afsluiten van apparatuur in bepaalde gevallen wel mogelijk, in weerwil van de tekst van de toelichting.

Combinatie technologieën (4G/DSL)

Bij de Stratix beschrijving van de combinatie 4G + DSL (door KPN hybrid access genoemd), het netwerktechnieken bij elkaar voegen om zo een grotere bandbreedte aan 'vaste' aansluitingen in bijvoorbeeld het buitengebied te kunnen realiseren, noemt Stratix Multipath TCP. In de praktijk is er meer nodig om twee verschillende media met verschillende kwaliteitskarakteristieken samen te voegen dan RFC 2684 beschrijft. Deze is dus ook niet voldoende als te publiceren specificatie van het demarcatiepunt. Er zijn feitelijk twee incompatibele implementaties van Huawei en Tessaes. Ook bij dit issue lijkt men in Duitsland zich niet bewust dat dit ook onder de nieuwe regelgeving zou kunnen vallen (bij DT heeft men de vergelijkbare oplossing 'Magenta Zu Hause').

Voor dit type oplossingen voor het buitengebied geldt dat deze experimenteel zijn, met waarschijnlijk een tijdelijke markt (tot bijvoorbeeld FttH in buitengebied meer gemeengoed is). Over het algemeen betreft het proprietary oplossingen van netwerkapparatuur-aanbieders die niet geïnteresseerd zijn in publicatie van de interfaces. Deze regel dwingt proprietary oplossingen die 'over het aansluitpunt heengaan' om protocollen te publiceren die aanbieders wellicht (nog) niet gepubliceerd wil zien. Hoe kleiner de markt, hoe lastiger dit is te bereiken.

E.5 Interviewverslag Tele2

Interview nav conceptrapport "Beleidsonderzoek modemkeuze - Analyse consultatiereacties betreffende technische implicaties vrije modemkeuze"

Tijdstip: donderdag 9 augustus 2018, 15:30h.

Locatie: Tele2, Wisselwerking, Diemen

Aanwezig: René Koning, Architect, datadiensten, Tele2

Alexander van 't Zand, regelgeving, Tele2

Bart Heinink, regulatory affairs, Tele2

Rudolf van der Berg, senior consultant, Stratix

Sietse van der Gaast, senior consultant, Stratix

E.5.1 Algemene indruk draft rapport

Tele2 deelt de interpretatie van het ministerie m.b.t. de regels niet. De beleidsregel is volgens Tele2 praktisch onuitvoerbaar en vormt een onzekere verplichting. Tele2 begrijpt dat het rapport beperkt van scope is en zich met name richt op technologische implicaties, maar wil toch aandacht vragen voor de effecten op haar bedrijfsvoering.

E.5.2 Specifieke punten

Tele2 noemt in het interview de volgende specifieke punten waarop ze nader zou willen ingaan:

1. Het (verplichte) monitoren van snelheden van 'offnet' klanten is niet langer mogelijk
2. Verlegging demarcatiepunt
3. Impact op VoIP
4. Impact op TV
5. Standaard APIs
6. Verantwoordelijkheden bij incompatibiliteitsissues

E.5.2.1 Offnet klanten niet monitoren

Op dit moment heeft Tele2 inzicht in de daadwerkelijke snelheden van de accessverbinding van klanten doordat Tele2 in de modems kan kijken. Dit kan niet meer als de modem niet meer door Tele2 bereikbaar is (offnet, als de DSLAM niet door Tele2 wordt beheerd). In dat geval is alleen nog de end-to-end verbinding met Tele2 te monitoren en niet op individuele snelheid want we hebben geen zicht op het stuk tussen modem en DSLAM. Deze DSLAM wordt namelijk beheerd door KPN, als deel van VULA (Virtual Unbundled Local Access) oplossingen. Snelheidsmetingen worden niet in de DSLAM (van KPN) gedaan.

Dus er zijn geen specifieke metingen mogelijk van de snelheid/capaciteit van de access lijnen. Zo is het volgens Tele2 niet langer mogelijk een betrouwbaar beeld van de daadwerkelijk te behalen snelheden te verkrijgen, terwijl dit wel verplicht is volgens andere regelgeving.

Na het interview stuurde Tele2 hierover op 14 september jl. nog enige aanvullende informatie, zie de bijlage bij dit interview.

E.5.2.2 Verlegging demarcatiepunt

'Verschuiving demarcatiepunt'

- EZ zegt: het verschuift niet, wij maken bestaande regelgeving alleen helderder
- Tele2 zegt: het demarcatiepunt verschuift wel ten opzichte van eerdere gangbare interpretaties van de regelgeving

Daarbij wil Tele2 opmerken dat nu een deel van de beveiliging in de modem zit. Dit zorgt ervoor dat het minder eenvoudig is om eigen apparatuur aan te sluiten en daardoor dat de klant niet rechtstreeks bij de Tele2 infrastructuur kan komen. Zij ziet de eigen modem keuze vanuit netwerk integriteit en veiligheid als het afbreken van een van de dijken die de Tele2 netwerken beschermen.

E.5.2.3 Impact op VoIP

SIP credentials zitten nu in het modem, als Tele2 deze aan de klant moet overdragen kan die klant de SIP service overal ter wereld gebruiken. Er zijn wel oplossingen om dit gebruik te beperken maar de impact daarvan is groot.

VoIP vrijgeven voor gebruik op andere apparaten vergt aanpassen van de dienst. Dat leidt bijvoorbeeld tot de mogelijkheid dat een gebruiker 10 parallele gesprekken opzet, dat soort zaken moet dan actief beperkt worden.

Bij misbruik van of over de Tele2 access-verbinding of van de credentials kan dan minder coulant worden opgetreden dan vandaag, omdat de verantwoordelijkheid verschuift naar de klant en de effecten groter zijn.

E.5.2.4 Impact op TV

Pragmatisch zou TV van de regelgeving uitgezonderd zijn (zoals ook in Duitsland het geval lijkt te zijn). Daarbij: is er eigenlijk wel een markt voor alternatieve set top boxen? Is deze situatie hoe dan ook niet van tijdelijke aard vanwege de markttrend naar over-the-top en software?

In Duitsland bieden fabrikanten (zoals AVM) 'specifieke firmware' voor operators . Problemen

Impact op TV is mogelijk beperkt. Toch mag daar de notie dat eigenlijk niks standaard is wel wat sterker.

Diensten zijn (nu) gekoppeld aan fysieke locatie. Als Tele2 dat straks gaat loskoppelen of de mogelijkheid creëert om die los te koppelen is volgens Tele2 die koppeling niet meer gegarandeerd en komt Tele2 mogelijk in problemen met rechtenhouders, die verplichten dat bepaalde diensten alleen op bepaalde locaties en/of via bepaalde apparaten mogen worden afgespeeld. De contracten van Tele2 staan bijvoorbeeld niet toe dat de TV-dienst op mobiele apparaten gebruikt wordt.

Na het interview stuurde Tele2 op 23 augustus jl. informatie over een aanvullend aandachtspunt op Set Top Boxen, zie hiervoor de bijlage bij dit interview.

E.5.2.5 Standaard APIs , proprietary APIs en veiligheidsaspecten

Beveiliging is belangrijk en het openbaar maken van ontwerpen, processen, gegevens en sleutels ziet Tele2 niet gebeuren. Maar zoals de regelgeving nu wordt uitgelegd wordt dit wel afgedwongen.

Er staat 'modems die de ISP's gebruiken zijn gemakkelijk verkrijgbaar voor consumenten'.

Modem is security demarcatiepunt voor ons (Tele2) en dat valt straks weg. Alle impact op systemen die daar direct achter zitten . Modem is laag 3 device dus laag 2 komt daar niet doorheen. Ook bijbehorende laag 2 attack factors komen niet daar doorheen.

Je faciliteert volgens Tele2 zo niet alleen de goedwillenden maar ook de kwaadwillenden. In een access domein raakt hij mogelijk andere klanten in hetzelfde access segment. In principe kan het mogelijk zijn dat de ene modem de andere modem bereikt. Hiertegen zijn zo goed mogelijk countermeasures genomen maar in het geval van een door Tele2 geleverde en beheerde modem sluit je dit issue volgens Tele2 uit.

E.5.2.6 Verantwoordelijkheid bij incompatibiliteitsissues bij standaardisatie.

Bij telefonie en vooral bij televisie geldt volgens Tele2 dat de gebruikte standaarden niet altijd leiden tot consistente implementaties door verschillende fabrikanten. Het is niet onmogelijk dat twee apparaten 'standaard compliant' zijn en er toch onvolkomenheden optreden in de communicatie daartussen. Tele2 vraagt Wie heeft welke rol in eventuele discussies daar over?

Met name het openstellen van de interface van TV diensten heeft mogelijk veel impact. Terwijl weinig partijen specifiek voor Tele2 een alternatieve set top box gaan ontwikkelen.

In de praktijk zal het dus vooral om alternatieve general purpose set top boxen gaan die worden aangeboden en afgenomen. Je moedigt daarmee mogelijk mensen aan om alternatieve modems te kopen en in te stellen die de impact en complexiteit daarvan mogelijk niet overzien.

E.5.a. Bijlage bij interviewverslag Tele2

Ontvangen op 23 augustus 2018:

Tekst Stratix paragraaf 5.3.2 van concept:

Tot voor een paar jaar geleden waren STBs specifiek voor een fabrikant of zelfs een telecom-bedrijf. Er zijn ontwikkelingen die er op wijzen dat de markt voor STBs die van de televisie en smartphone volgt, met vergelijkbare chipsets en besturingssystemen. Android TV en Apple TV worden soms al op deze wijze ingezet.³⁷ Dit maakt het mogelijk voor telecombedrijven om de apps die ze voor tablets en smartphones ontwikkelen geheel of gedeeltelijk te hergebruiken voor STBs. Wil een fabrikant een concurrerende STB in de markt zetten, dan zal deze de combinatie van hardware, software, DRM en andere functionaliteit moeten ondersteunen, welke functioneel tot een diep niveau niet te onderscheiden is van die van de aanbieder.

Als de consument zelf een set top box moet kunnen kiezen, dan is de eerste vraag hoeveel van de functionaliteit ondersteund moet kunnen worden. Als het alleen gaat om het en selecteren en bekijken van televisiestreams over IPTV of kabel dan lijkt dat nog wel mogelijk. Op een kabelnetwerk worden de belangrijkste kanalen altijd uitgezonden en kunnen andere kanalen op verzoek bijgeschakeld worden. Hiervoor zijn standaarden beschikbaar. Ook voor IPTV geldt ook dat het activeren van een stream een standaard volgt. Het kijken van traditionele lineaire televisie lijkt dus mogelijk en te ondersteunen, mits IPTV aanbieders publiceren welke standaarden ze gebruiken en hoe deze geïmplementeerd zijn.

Opmerking Tele2:

Hier lijken twee ontwikkelingen tegelijk besproken te worden waardoor een verkeerde indruk kan ontstaan. De indruk lijkt gewekt te worden dat er ontwikkeling is waardoor proprietary IP TV oplossingen van een aanbieder ook op andere STBs ter beschikking komen. Wat je er ook van vindt, het tegendeel is waar.

Volgens Tele2 zou hier duidelijker naar voren kunnen dat i) van zo'n ontwikkeling geen sprake is en ii) dat er bij proprietary IP TV wel degelijk een probleem is juist omdat er geen of beperkt sprake is van standaarden. Het zal dus een enorme effort vergen om een beschrijving te geven van relevante specificaties; iii) Stratix staat niet stil bij een mogelijke demarcatie tussen specs die je moet leveren op basis van de beleidsregels en specs die niet geleverd hoeven worden, bijvoorbeeld omdat er een OTT dienst geïntegreerd op de STB wordt geleverd.

Ontvangen op 14 september 2018:

Aanvullende opmerking Tele2:

Wat ons betreft hebben we in het interview te weinig aandacht gegeven aan het wegvallen de controle over de eind tot eind verbinding bij vrije modemkeuze.

Daarbij zijn de aspecten veiligheid en, het Tele2 specifieke issue van off net klanten aan bod gekomen. En deze punten zijn terecht maar Tele2 hecht eraan te benadrukken dat dit slechts 2 aspecten zijn. Daarnaast vraagt Tele2 ook aandacht voor Snelheid en QoS;

- Het end-to-end beheer van de verbinding valt weg of wordt beperkt waardoor de quality of service niet voldoende gemonitord kan worden en daarmee ook niet gegarandeerd.
- Dat zelfde geldt voor snelheid. De snelheid die Tele2 kan garanderen op haar eigen modems kan ze niet garanderen op modems van derden. Afgezien van de specs, die al dan niet voldoende zijn om de optimale snelheid te halen, geldt dat Tele2 de snelheid op de modem niet meer kan meten. En om die reden dus ook niet garanderen op de manier waarop ze dat wel kan op eigen modems

E.6 Interviewverslag T-Mobile

Interview n.a.v. conceptrapport "Beleidsonderzoek modemkeuze - Analyse consultatiereacties betreffende technische implicaties vrije modemkeuze"

Tijdstip: dinsdag 11 september, 9:30h.
Locatie: T-Mobile, Den Haag
Aanwezig: Frank van Berkel, Senior regulatory counsel T-Mobile,
Michael van Dooren, Solution architect T-Mobile,
Frank de Caluwé, Security planning en engineering lead T-Mobile,
Rudolf van der Berg, senior consultant, Stratix,
Sietse van der Gaast, senior consultant, Stratix.

E.6.1 Algemene indruk draft rapport

Het draft rapport werd door T-Mobile 'grotendeels OK' genoemd. De titel van het rapport was voor T-Mobile wel enigszins bevreemdend: waarom de titel "Beleidsonderzoek modemkeuze" gekozen terwijl het netwerkaansluitpunt de discussie was. Stratix legde uit dat de onderzoeks-aanvraag door EZK zo genoemd is maar dat de voorgenomen beleidsregel inderdaad bredere implicaties heeft die ook in de consultatiereacties en het rapport naar voren komen.

T-Mobile geeft aan dat ze in het algemeen bezorgd zijn dat het juridisch kader van bestaande wet- en regelgeving wordt veranderd onder het mom beleidsregel. In feite is de regelgeving er al sinds 2008 en wordt er nu pas invulling aan gegeven. Je kunt zelfs teruggrijpen op besluiten sinds 1989 over het aansluitpunt waar meermalen invulling aan is gegeven om toepasbaar te kunnen blijven op nieuwere technologieën.

De aankondiging uit 2016 van EZK om vrije apparaat keuze scherper af te bakenen in een beleidsregel was ook voor T-Mobile een verrassing. De voorliggende uitwerking zal voor operators, en dus ook voor T-Mobile, een behoorlijk grote impact hebben:

- Operators moeten zich instellen op veel meer klantvragen waar het lastig is antwoorden op te geven, en waarbij voor een groot deel ook zal moeten worden gewezen op de eigen verantwoordelijkheid. Waar nu in veel gevallen kan worden meegekeken met een klant in problemen kan dat straks soms niet meer. Zullen het vooral de technisch vaardigen zijn die een eigen modem gaan installeren of juist niet? En de technisch vaardigen zijn theoretisch weliswaar ook het meest zelfredzaam maar vaak ook de klanten die het meest doorvragen.
- De flexibiliteit voor een operator om in bepaalde gevallen af te wijken van algemene specificaties wordt geminimaliseerd. T-Mobile vraagt in sommige gevallen fabrikanten af te wijken van RFCs omdat dit bijvoorbeeld de veiligheid of betrouwbaarheid van het netwerk verhoogt. Zo is er een DHCP process waarin een bepaald backoff / retry mechanisme zit. Als DHCP geen antwoord krijgt, dan vraagt het iedere seconde opnieuw om een IP-adres. Dit zou in sommige gevallen tot een bijna DDOS achtige situatie leiden. Vandaar dat T-Mobile fabrikanten van routers vraagt om dit anders in te richten.
- Er moeten specificaties gepubliceerd worden. Maar EZK zal heel goed moeten nadenken hoe ver deze specificaties zullen moeten gaan en ook welke eventuele tegenacties

(inclusief afsluiten) kunnen worden verwacht bij niet voldoen aan de door operator gepubliceerde specificaties.

De klant loopt ook een risico met de keuze voor een eigen modem, betoogt T-Mobile, en een operator zal dat risico dan ook bij de klant willen (en moeten) leggen want anders wordt het onwerkbaar. T-Mobile heeft uiteraard via haar Duitse partner al wat ervaring met dergelijke wetgeving en er zijn wel wat implicaties, ook onverwacht. Bijvoorbeeld mensen die 10 jaar oude modems gebruiken, die niet meer worden ondersteund en dus zeer kwetsbaar zijn.

E.6.2 Specifieke punten

Een aantal specifieke issues en complexiteiten werden besproken:

1. Professionele diensten over consumentenaansluitingen
2. Credentials en fraude SIP gegevens
3. Scheiding en toewijzen / verwijzen verantwoordelijkheden niet helder
4. Timing invoering
5. Uitrol en uitvoeren updates wordt complexer
6. Verplichte publicatie haalbare snelheid
7. Toename juridisering
8. TV set top box

Hieronder worden de besproken issues kort samengevat.

E.6.2.1 Professionele diensten over consumentenaansluitingen

Eén van de problemen die T-Mobile signaleert en die door de nieuwe wetgeving zal worden verergerd is dat veel bedrijven professionele diensten proberen te draaien via consumenten aansluitingen en consumenten abonnementen en naar eigen inzicht consumentenapparatuur gaan inzetten. T-Mobile vindt dat lastig want de verbinding is daar helemaal niet voor bedoeld en het levert veel klantvragen op.

Dit alles gaat ook ten koste van customer experience en van flexibiliteit van (netwerk)aanbieders. T-Mobile vraagt zich af in hoeverre ze nog vrij zijn om eigen diensten te ontwikkelen.

Eén en ander zal ook leiden tot een waterbedeffect: de nieuwe situatie zal de operators weer nopen tot meer specificaties en regels en dit zal leiden tot andere effecten die ook weer gereguleerd moeten worden.

E.6.2.2 Credentials en fraude SIP gegevens en hacken klantapparatuur

Op dit moment houdt T-Mobile de SIP gegevens geheim voor de klanten. Met deze gegevens kan in verkeerde handen namelijk misbruik gepleegd worden, bijvoorbeeld automatisch bellen op naam van de klant. Op dit moment neemt T-Mobile bij misbruik in veel gevallen de kosten van bijvoorbeeld automatisch bellen voor eigen rekening, maar als die credentials aan de klant zijn verstrekt omdat men zelf een SIP server wil kopen en beheren is men zelf verantwoordelijk voor de credentials. SIP-fraude is in de zakelijke markt al een bekend probleem. Als consumenten hun eigen SIP-verbindingen kunnen maken, dan is het redelijk te verwachten dat de fraude ook toe zal nemen. Vrijheid komt met verantwoordelijkheid. Iets dergelijks geldt voor het gebruik van verouderde apparatuur.

Modems en andere apparatuur kan worden gehackt en overgenomen. Hiervan zijn voorbeelden bekend zowel wereldwijd (Brazilië) als dichtbij. Het draft rapport noemt voorbeelden hiervan en mogelijke indirecte gevolgen zoals het stelen van creditcard gegevens.

E.6.2.3 Scheiding en toewijzen / verwijzen verantwoordelijkheden niet helder

Sommige consequenties van de beoogde beleidsregel zijn nog niet helder. Het is duidelijk dat bij een zelfgekozen modem meer verantwoordelijkheid bij de eindgebruiker komt te liggen, maar waar de verantwoordelijkheid van de aanbieder ophoudt en die van de klant begint is soms niet zo simpel vast te stellen. Als bijvoorbeeld een niet-T-Mobile modem gehackt is wat zijn dan de verantwoordelijkheden ten aanzien van publicatie van de hack en mogelijke tegenmaatregelen?

De back office van T-Mobile krijgt hoe dan ook klantvragen te verwerken, ook al gaan ze die niet beantwoorden of ligt het beantwoorden er van buiten de verantwoordelijkheid van T-Mobile. Er is hoe dan ook toch angst voor reputatieschade voor T-Mobile.

E.6.2.4 Timing invoering

T-Mobile vindt het belangrijk dat de beleidsregel niet overhaast wordt geïntroduceerd, en dat er goed overleg is met de sector en betrokken andere overheidsinstanties. Aan de ene kant zegt EZ dat apparaten veiliger (IoT) moeten worden. Aan de andere kant zegt EZK dat je zoveel mogelijk apparaten kunnen gebruiken. Hier zit een bepaald dilemma. T-Mobile vraagt zich af hoe EZ de veiligheid van de apparaten, met name bij de fabrikanten, gaat afdwingen. T-Mobile zegt wel verantwoordelijkheid te kunnen nemen voor de apparaten die ze zelf uitlevert, maar niet voor die apparaten waarover ze geen invloed kan uitoefenen. Die verantwoordelijkheid moet volgens T-Mobile elders, bij de fabrikant of de gebruiker, worden neergelegd.

Fabrikanten zullen er zich rekenschap van moeten geven dat bij fouten in apparatuur en firmware negatieve beeldvorming ook op hen kan afstralen: bij de nieuwe regelgeving zal de bal sneller bij fabrikanten gelegd worden. Zelfs als 'vrije apparatuur keuze' een valide punt is van consumenten en apparatuur fabrikanten is het belangrijk dat alle stakeholders beseffen dat het niet even snel geregeld kan worden. T-Mobile pleit er voor om hiervoor voldoende tijd te nemen en dit marktbreed aan te pakken.

E.6.2.5 Complexiteit uitrol en uitvoeren van updates neemt toe

T-Mobile betoogt dat met de nieuwe regelgeving je de problematiek rond up to date houden van apparatuur, firmware en software die nu bij mobiele telefoons en smartphones speelt ook bij de vaste lijnen gaat introduceren. Gedoeld wordt op de discussie rond ondersteuning van operating systemen en updates van firmware van telefoons die een aantal jaren in het bezit zijn van consumenten.

Vragen die daar volgens T-Mobile onder andere bij opkomen zijn: Wie is verantwoordelijk voor de 'customer life cycle'? Mag je eisen dat een klantmodem wel onder support van een andere partij staat?

E.6.2.6 Verplicht publiceren van haalbare snelheid (netneutraliteitsregels)

ACM heeft regels opgesteld over het verplicht publiceren van de datasnelheid die gehaald kan worden op een aansluiting. Dit werkt met een gecertificeerde BEREC methode. Hoe werkt dit als klanten zelf alternatieve apparatuur kan plaatsen? Dit issue wordt genoemd in rapport maar T-Mobile wil dit graag nogmaals onder de aandacht brengen. T-Mobile ziet dit als

onderdeel van de netneutraliteitswetgeving, en vreest dat daarbij om het in overeenstemming te brengen met de nieuwe beleidsregel veel disclaimers nodig zullen zijn met betrekking tot situaties waarbij eigen apparatuur gebruikt wordt. T-Mobile vraagt zich af wat uiteindelijk dan het nut nog zal zijn van de verplichting tot publiceren van de snelheid. Het nut zal volgens T-Mobile in elk geval afnemen, omdat de transparantie minder wordt.

Er is een veeleisend deel van de klanten die zowel graag een eigen modem plaatst alsook de aanbieder houdt aan de geadverteerde snelheden. Dit kan mogelijk discussies opleveren.

T-Mobile voorziet daarbij onder andere discussies tussen klanten en de helpdesk: stel een klant heeft alle profielen goed gezet en haalt toch de geadverteerde snelheid niet. Bijvoorbeeld omdat er toch een mismatch is tussen de klantmodem en de centrale apparatuur. Moet T-Mobile dan aantonen dat er een fout is in de chipset van het bewuste modem en/of de DSLAM? Of ligt de bewijslast bij de consument?

E.6.2.7 Vrije modemkeuze leidt tot onnodige juridisering

Welke garanties wel en niet haalbaar zijn met een eigen modem leidt tot een enorme extra juridisering. Een aantal voorbeelden zijn hierboven al genoemd. Ook kan het in vele opzichten mogelijk perverse prikkels opleveren. Bijvoorbeeld de kwestie of er wel of niet voor een operatormodem betaald moet worden.

E.6.2.8 TV set top box

T-Mobile vindt dat de vrije set top box keuze voor TV een heel ander issue is dan de vrije modemkeuze. Effectiever zou het volgens T-Mobile zijn als EZ de decoder-regulering (voorwaardelijke toegang, hoofdstuk 8 Tw) weer van stal zou halen, met bijzondere toegang tot de decoder.

T-Mobile betoogt dat er zo veel specifieke software en maatwerk in hun set top box zit dat het heel lastig wordt om dat allemaal vrij te geven of een te publiceren interface hiervoor te maken. 'Het openen van set top boxen is eigenlijk zonde van je tijd'. Op termijn gaat software de rol van set top boxen overnemen.

Ook werd nogmaals genoemd dat de content aanbieders hier een essentiële rol spelen: niet alle specificaties mogen door T-Mobile zomaar worden vrijgegeven en interfaces mogen niet zomaar worden opengezet zonder toestemming van de rechthebbenden.

E.7 Interviewverslag VodafoneZiggo

Interview n.a.v. conceptrapport "Beleidsonderzoek modemkeuze - Analyse consultatiereacties betreffende technische implicaties vrije modemkeuze"

Tijdstip: donderdag 16 augustus 2018, 14:00h.

Locatie: VodafoneZiggo, Kabelweg 51, Amsterdam

Aanwezig: Rene Blanckstein, government security affairs manager, VodafoneZiggo

Walter Kroeze, manager regulatory affairs, VodafoneZiggo

Jeroen den Haan, product & program implementations, VodafoneZiggo

Edwin Kamphuis, design en deployment inhome & residential, VodafoneZiggo

Hind Abdulaziz, consultant, Stratix

Sietse van der Gaast, senior consultant, Stratix

E.7.1 Algemene indruk draft rapport

VodafoneZiggo heeft als voorbereiding op dit interview en naar aanleiding van het verstuurd draft rapport ook een schriftelijke reactie voorbereid en zegt deze de volgende dag naar zowel Stratix als het Ministerie van Economische Zaken en Klimaat te zullen mailen. Deze schriftelijke reactie is wat VodafoneZiggo betreft vollediger dan de onderwerpen die in het tijdsbestek van een interview aan de orde kunnen komen omdat daar de argumentatie met betrekking tot de voorgenomen Beleidsregel het meest uitgebreid en correct wordt weergegeven.

De door Stratix naderhand op 17 augustus 2018 ontvangen schriftelijke reactie is bijgevoegd als bijlage aan dit interviewverslag.

Om de algemene indruk te kenschetsen werden door VodafoneZiggo een aantal punten opgesomd:

- De voorgenomen beleidsregel heeft een grote impact op de business van VodafoneZiggo (security, administratieve processen, klantenservice) en op die van klanten
- Binnen Europa draagt de nieuwe Europese Elektronische Communicatie Code (die in de loop van 2020 in werking treedt) aan BEREC op om richtsnoeren op te stellen met betrekking tot de definitie van netwerkaansluitpunt bij verschillende technologieën.
- Concrete regelgeving op het gebied van modemkeuze is er voor zover VodafoneZiggo weet op dit moment alleen in Duitsland. Bij Liberty Global, het moederbedrijf van Ziggo, zijn er geen signalen van voornemens tot dergelijke regelgeving in andere landen. Set Top Boxen zijn – voor zover bekend – geen onderdeel van de regelgeving in Duitsland.
- VodafoneZiggo wil geen rare Dutch special, en vindt het onverstandig om in Nederland vooruit te lopen met een ingrijpende aanpassing van lopend beleid waarvan niet duidelijk is of die met de toekomstige invulling overeenkomt.
- Eén en ander heeft volgens VodafoneZiggo ook invloed op ander beleid, zoals beleid rond security en de maatschappelijke verantwoording van VodafoneZiggo over veiligheid naar onze klanten toe.

- In Duitsland, blijkt maar 1 à 2 % van de klanten uiteindelijk gebruik te maken van de mogelijkheden die de nieuwe regelgeving daar biedt en gebruikt eigen apparatuur in plaats van de door de provider geleverde apparatuur. En een deel daarvan komt uiteindelijk weer terug, en maakt inmiddels alsnog weer gebruik van de apparatuur die door de provider geleverd wordt.
- VodafoneZiggo vindt het belangrijk dat de argumenten in de discussie over het netwerkaansluitpunt goed verwoord worden, met de relevante voors en tegens, vandaar dat zij ook een schriftelijke reactie op het concept rapport heeft opgesteld.
- Wat betreft Set Top Boxen onderkent Stratix dat vrije keuze voor problemen gaat zorgen maar dit komt volgens VodafoneZiggo niet voldoende tot uitdrukking in de eindconclusies.

De conclusies in het Stratix draft rapport worden volgens VodafoneZiggo veelal op basis van aannames en verwachtingen gedaan, in plaats van op feiten gebaseerd. Een concreet voorbeeld hiervan is volgens VodafoneZiggo de veronderstelling van Stratix dat gebruikers ook regelmatig zelf de software van hun apparatuur zullen updaten. Een onderbouwing hiervan ontbreekt. VodafoneZiggo verwijst naar een Engels onderzoek naar routers waaruit blijkt dat in de praktijk maar 11-14% van de gebruikers regelmatig een update doet. De rest laat het lopen.

Een algemene zorg van VodafoneZiggo zijn de definities. Vaak wordt het woord modem gebruikt waar soms modem functionaliteit wordt bedoeld maar soms de combinatie modem/router of op andere plaatsen modem/router/wifi access point. Stratix herkent zich hier deels in. Het is belangrijk de functionaliteiten goed te onderscheiden en te benoemen. On met name hoofdstuk 3 wordt daarom geprobeerd de verschillende functionaliteiten die in de door operators aangeboden dozen wordt gevat uit elkaar te trekken en afzonderlijk te beschrijven. Toch wordt in veel situaties, en ook in veel consultatiereacties – ook door operators – vaak over ‘het modem’ gesproken waar de doos met het totaal van functionaliteiten wordt bedoeld. VodafoneZiggo bedoelt met “Modem” het apparaat wat het Docsis signaal omzet in een internet-toegangsdienst (IPv4/IPv6). Een “Router” is het apparaat dat de internettoegangsdienst verbindt met een lokaal thuis netwerk. De router kan verschillende features bevatten zoals wifi, firewalls, etc.

VodafoneZiggo ziet dat Stratix in het draft rapport lijkt te concluderen dat het opnemen van set top boxen (STBs) onder de werking van de Beleidsregel gaat leiden tot complexe situaties, waaronder met betrekking tot Digital Rights Management (DRM) en additionele functionaliteiten. VodafoneZiggo leest hierin dat Stratix concludeert dat het opnemen van STBs onder de werking van de regel geen goed idee is. In de eindconclusie wordt hierover echter niets gezegd.

Verschillende sub-hoofdstukken in het draft rapport beschrijven zorgen en problemen als gevolg van vrije modemkeuze, maar in de eindconclusie mist VodafoneZiggo die nuance waardoor deze positiever wordt dan de rest van het rapport. Dit verschil verbaast VodafoneZiggo enigszins.

E.7.2 Specifieke punten

Voor alle specifieke onderwerpen verwijst VodafoneZiggo naar de schriftelijke reactie op het concept rapport van Stratix van VodafoneZiggo, 16 augustus 2018, door Stratix ontvangen de dag na het interview (zie bijlage).

VodafoneZiggo gaf aan het draft rapport graag per hoofdstuk te bespreken. Hierbij werden bij een aantal paragrafen of hoofdstukken bepaalde onderwerpen besproken, waarbij VodafoneZiggo kanttekeningen plaatst of toelichting geeft bij de teksten in het draft rapport.

Globaal werden tijdens het interview de volgende paragrafen en onderwerpen besproken:

- 5.1. Impact op operator netwerk
 - o Standaarden en praktijk
 - o Shared medium effecten door modems met oudere Docsis varianten
 - o Interferentie
 - o Firmware updates
- 5.2. Issues rond impact veiligheid
 - o Puma chipset issue
 - o Firewall beheer
- 5.3 Impact op diensten
 - o Set Top Boxen (STBs)
 - o Mobiel (femtocellen)
- 5.4. Impact rond issues eigen apparatuur
 - o Conclusies eigen netwerk en eigen apparatuur
- 6. Impact consumenten
 - o Impact consumenten

Hieronder worden de discussies rond deze onderwerpen kort beschreven.

E.7.2.1 Over 5.1. "issues rond impact op operator netwerk"

In Hoofdstuk 5.1 van het draft rapport staat:

"Aangezien de aanbieders veelal geen uniform netwerk hebben, zullen ze sowieso naar een veelheid van modems moeten kijken. Ook in dit opzicht is er geen verandering voor de situatie van andere aansluitingen. De vrije modemkeuze zal als zodanig dan geen grote risico's met zich meebrengen. Wel zullen de aanbieders een administratief proces moeten inrichten om de modems van klanten te registreren en activeren in het netwerk."

VodafoneZiggo merkt hierover op: De conclusie van Stratix dat de vrije modemkeuze als zodanig geen grote risico's met zich zal meebrengen is gebaseerd op indrukken en inschattingen. Vanuit Duitsland zijn de conclusies uit de praktijk dat er zich wel degelijk problemen voordoen. We hebben nu inderdaad ook al een veelheid aan modems in onze netwerken, onder andere vanwege de historie van onze netwerken en de evolutie naar de support van nieuwere Docsis varianten, maar we hebben heel hard gewerkt om de interoperabiliteit goed te laten verlopen. Daarbij zijn bijvoorbeeld per netwerktype en/of locatie bepaalde modemtypen die worden ge-support. Niet alle modems werken overal even goed.

Standaarden in praktijk

De Docsis standaarden zijn er, maar de implementaties daarvan zijn niet zo strikt. Bij introductie van een nieuwe modem is VodafoneZiggo minimaal 1 jaar bezig om het werkbaar te maken. Daarnaast is het een on-going proces, o.a. om firmware updates van de modems te testen en te introduceren.

De IP standaarden van IPv4 en IPv6 (dus van de routers) zijn veel strikter en beter dan modemstandaarden (zoals Docsis en (V)DSL) en daarom kan je gewoon bij de mediamarkt wel een WiFi router kopen en zonder problemen in gebruik nemen en niet zo maar een modem.

Ondanks de interoperability testing, komt het voor dat een modem niet goed werkt. Dat is de realiteit van nu. En dit gebeurt soms al met de gerenommeerde merken, waarbij er al een relatie is tussen netwerk operator en modemfabrikant.

Als de voorgenomen beleidsregel doorgezet wordt, komen er volgens VodafoneZiggo modems van onbekende fabrikanten, waar geen relatie mee bestaat, bij met het gevaar dat na updates niets meer werkt, of is er een groter risico.

Nu kan je je VodafoneZiggo modem al in bridge modus zetten, waar je je eigen netwerk door middel van een WiFi router achter kunt zetten. In het modem zitten in deze modus geen extra features behalve dat de kale Docsis signalen naar een internettoegangsdienst worden omgezet. Het standpunt van VodafoneZiggo is dat er hiermee al voldaan wordt aan de vrije apparatuur keuze voor de consument.

Shared medium effecten door modems met oudere Docsis varianten

Kabel is een shared medium, dus als één modem iets niet goed doet, is het moeilijk te detecteren waar het fout gaat. Impact is dan op het hele wijk. Dit is anders dan DSL. De invloed van oude modems is volgens VodafoneZiggo aanzienlijk: deze gebruiken bijvoorbeeld minder (TV)kanalen om het datasignaal over te transporteren. Als oude types maar 1 of 4 kanalen gebruiken kunnen deze door andere modems niet meer gebruikt worden. Dit heeft uiteindelijk invloed op de maximale bandbreedte die verdeeld kan worden over een groep modems. Dit kan zeker bij introductie van Docsis 3.1 een issue worden.

Interferentie

Volgens VodafoneZiggo heeft een oud modem, dat niet goed is afgeschermd is, mogelijk invloed op andere modems in een wijk. Het gaat hier niet om instraling door antennes want dit heeft alleen lokaal invloed en is dus minder relevant voor dit onderwerp, maar om storingen van één modem die overspraak/interferentie geven op andere delen van het netwerk.

Firmware updates

Firmware updates kunnen volgens de standaard alleen via docsis ge-update worden. De klant thuis mag dit niet vanuit huis doen. Indien de modem ook onder vrije apparaatkeuze valt, en deze niet de juiste updates gehad heeft, zal VodafoneZiggo bij veiligheids issues de gebruiker moeten afsluiten omdat een modem misschien niet de juiste updates heeft gehad. Modems die niet door VodafoneZiggo zijn geïnstalleerd moeten door gebruikers op andere manieren worden ge-update. Dit is niet triviaal, de modem zal dan bijvoorbeeld opgestuurd moeten worden naar de modem leverancier.

Volgens de Docsis specificaties kan een kabelbedrijf de firmware versie van een modem uitlezen, zodat ook op die manier modems kunnen worden geïdentificeerd en geïsoleerd. Maar dit uitlezen werkt niet altijd bij alternatieve modems.

Het enige dat VodafoneZiggo in een geval van een veiligheid issue bij een 'eigen' modem kan doen is het modem (en dus de klant) afsluiten. Ze kunnen de klant niet meer helpen.

Kortom: VodafoneZiggo staat achter de bridge modus variant, ziet het modem als onderdeel van het netwerk en ziet bellen op de weg als de modemkeuze opengegooid wordt op de manier die EZK nu voorstaat.

Een vermeldenswaardig incident is een veiligheidsprobleem in Nederland doordat in Duitsland de modemkeuze is vrijgegeven. Er is een veiligheidsprobleem ontstaan in één van de vrije modem modellen die in Duitsland is gebruikt en dit heeft invloed gehad op andere kabelnetwerken ter wereld, ook in Nederland. Het veiligheidsprobleem maakte mogelijk dat een bedrijfje illegaal Ziggo producten en diensten doorverkocht (door zgn "modem cloning").

E.7.2.2 Over 5.2 "Issues rond impact op veiligheid"

VodafoneZiggo deelt het relatieve optimisme in het draft rapport over de kennis en vaardigheid van de klanten niet.

Puma chipset issue

In paragraaf 5.2.2 van het rapport staat bijvoorbeeld: *Een bekend recent probleem zat in opeenvolgende generaties van de Puma 5, 6 en 7 processoren van Intel voor kabelmodems. Deze zijn de basis zijn van kabelmodems van Comcast, Virgin UK en VodafoneZiggo. Deze processoren hadden een probleem waardoor de latency van pakketten zeer hoog kon worden³⁰. Dit effect trad al op bij dagelijks gebruik en leidde tot veel klachten van eindgebruikers. Alhoewel de basis van het probleem al in 2016 gedocumenteerd was, werd de volle omvang ervan in 2017 wereldwijd duidelijk. Vanuit veiligheidsoogpunt is relevant dat al in april 2017 bekend werd dat een stroom pakketten van ongeveer 200kbps in principe in staat was om een kabelmodem onbereikbaar te maken. Het effect is een zogenaamde "Denial of Service"-attack. VodafoneZiggo verwachtte pas in april 2018 een patch te kunnen hebben. [...] Ziggo-gebruikers adviseerden elkaar op discussieforums als Tweakers om over te stappen naar een andere modem, zonder Intel chipset.*

Dit betrof een probleem van slechts enkele tientallen gebruikers op de 1 miljoen gebruikers van dit type modem. Er is een hele kleine groep gebruikers die veel eisen hebben en soms extra functionaliteit behoeven. Dit gaat om minder dan 5 gevallen per maand. Veelal probeert VodafoneZiggo deze high end user group ook in een soort testgroep van 'friendly users group' in te zetten bij nieuwe ontwikkelingen.

Over het algemeen zijn firmware updates juist vrij tijdrovend. Het kost een jaar testen om fouten en veiligheidsissues zo veel mogelijk uit te sluiten, pas daarna kan firmware ge-update worden naar miljoenen klanten. Hier zijn bovendien enkele varianten in te onderscheiden: VodafoneZiggo hanteert een actief multi-vendor beleid met verschillende modemtypen, je zit altijd met evolutiepaden waarbij delen van het netwerk al zijn gemigreerd naar een nieuwe standaard en anderen niet, en ook zijn Ziggo en UPC netwerken zijn nog niet technisch helemaal hetzelfde.

Firewall beheer

In paragraaf 5.2.2 van het draft rapport staat: *"Firewall beheer operators heeft op dit moment niet veel meerwaarde..."*

Hier is mogelijk enige verwarring over de achtergrond van deze bewering. VodafoneZiggo stelt: de klant kan zijn eigen router achter die van VodafoneZiggo zetten door de VodafoneZiggo

modem+router combinatie in bridge modus te zetten. Maar ook zonder bridge modus heeft de klant een vrije keuze in bijvoorbeeld kinder filters, via OpenDNS en andere DNS aanbieders. De klant kan hierdoor (ook in de huidige situatie) los van het modem zijn eigen keuzes maken.

Stratix heeft met deze opmerking vooral bedoeld dat firewall beheer door de operators in de door operators geleverde modem/router op dit moment niet veel meerwaarde heeft.

E.7.2.3 Over 5.3: "Issues rond impact op diensten"

Set top Boxen (STBs)

Bij Set Top Boxen hanteert VodafoneZiggo al een vrije marktmodel. Klanten kunnen al ontvangers en televisies kopen die zonder problemen op ons netwerk aangesloten en gebruikt kunnen worden. Zodra deze gecertificeerd zijn door VodafoneZiggo wordt gegarandeerd dat ze probleemloos werken. Als bedrijf steken we ook veel tijd en budget in dit certificeringsproces.

Sommige van de VodafoneZiggo diensten (TV, DRM) kunnen alleen op onze eigen set top boxen aangeboden worden. Als de klant een eigen STB boxje heeft, dan kan hij beperkte functionaliteit krijgen die door dat boxje wordt ondersteund, bijvoorbeeld lineaire TV. Het strekt zeer ver om alle VodafoneZiggo specifieke functionaliteit en de bijbehorende interfaces te specificeren en publiceren.

Er wordt (ook in het rapport) gezegd dat er een algemene trend naar over-the-top diensten (over IPv4/IPv6 internet) is en dat operator specifieke Set Top Boxen op termijn waarschijnlijk zullen verdwijnen.

Als dit klopt, waarom dan nu iets optuigen waarbij de Set Top Boxen met allerlei ingewikkelde maatregelen worden omgeven, terwijl het gebruik hiervan hoe dan ook op termijn een aflopend verhaal zal zijn?

Mobiel (femtocellen)

In paragraaf 5.3.2 van het draft rapport worden opmerkingen gemaakt over overige (publieke) diensten, waaronder het aansluiten van femtocellen via thuis- of bedrijfsnetwerken. VodafoneZiggo benadrukt dat repeaters, picocellen en/of femtocellen alleen aangesloten mogen worden met toestemming van de betreffende mobiele operator. Eigen zendapparatuur kan alleen geplaatst en aangesloten worden bij gebruik van ongelicenseerde banden, als daar geen operator bij betrokken is.

Stratix is het met die uitleg eens, maar denkt dat dit verder niet gerelateerd is aan het issue van de vrije modem/router keuze. Een picocel van operator M moet ook via een access netwerk van een andere operator V kunnen worden aangesloten zonder dat dit apparaat als onderdeel wordt gezien van het netwerk van operator V. Maar de cel is natuurlijk wel onderdeel van het netwerk van operator M en er dient door operator M toestemming voor het gebruik van de frequenties te worden gegeven.

De opmerkingen van VodafoneZiggo hebben onder andere de volgende achtergrond:

- Femtocellen werden in het verleden aangeboden aan klanten met een slechte mobiele thuisdekking. Deze 3G celletjes gebruikten heel weinig zendvermogen en hoefden

daarom niet als onderdeel van het mobiele radio access netwerk opgenomen te worden in de radioplanning. Al een aantal jaren worden femtocellen niet meer aangeboden. Wel worden op dit moment door VodafoneZiggo picocellen aangeboden, die als onderdeel van het mobiele radio access netwerk wel opgenomen worden in de radioplanning. VodafoneZiggo suggereert bijvoorbeeld de term 'kleine basisstations' te gebruiken ipv het niet juiste femtocellen.

- Sommige bedrijven lever(d)en repeaters aan bedrijven en particulieren. Het gebruik van deze repeaters zonder toestemming van de operator is illegaal omdat dan gebruik gemaakt wordt van aan VodafoneZiggo gelicenseerd spectrum. Agentschap Telecom ziet hier scherp op toe omdat illegaal gebruik van de apparatuur storing kan veroorzaken en de bereikbaarheid van 112 in gevaar kan brengen.

E.7.2.4 Over 5.4 "Issues rond impact op eigen netwerk en eigen apparatuur"

Conclusies eigen netwerk en eigen apparatuur

In het Stratix draft rapport staat: *"Een vrije routerkeuze zal geen negatieve effecten hebben op het functioneren van het interne netwerk en het netwerk van de telecomaandbieder. Het zal consumenten wel meer mogelijkheden geven hun interne netwerk vorm te geven. Aanbieders mogen geïntegreerde oplossingen blijven aanbieden. De vrije modemkeuze zal het echter moeilijker maken om de gehele infrastructuur te controleren."*

VodafoneZiggo is het eens dat het controleren ofwel het beheer lastiger wordt in dat geval, maar vraagt zich ook en vooral af of het de klant wel helpt. Daarnaast kan de klant zijn eigen interne netwerk ook nu immers al volledig vorm geven met een eigen router, die hij op een in bridge modus gezet modem van VodafoneZiggo kan aansluiten.

E.7.2.5 Over 6 "Analyse beheersbaarheid"

Impact consumenten

Hier staat in het Stratix draft rapport: *Het is maar zeer de vraag hoe gebruikers zullen reageren op de vrije modemkeuze. Verwacht kan worden dat de marktwerking hier zijn werk zal doen. Als de aanbieders een modem/router leveren die door de gebruikers als goed genoeg beoordeeld wordt, dan zal er weinig animo zijn om een ander apparaat te gebruiken. Mocht de aanbieder echter een modem/router gebruiken die voor problemen zorgt, dan hebben gebruikers meer de neiging om over te stappen.*

Hierbij stelt VodafoneZiggo vooral de proportionaliteit ter discussie, en wijst op de getallen in Duitsland van het percentage daadwerkelijke overstappers naar een eigen modem, en de moeite die het kost om te voldoen aan de maatregel.

In Nederland gebruikt tussen 5 en 10% van de VodafoneZiggo klanten de bridge modus. Er is dus een kleine maar niet onaanzienlijke minderheid met de behoefte om zelf alternatieve apparatuur thuis te kunnen plaatsen. VodafoneZiggo vindt dat ze door de bridge modus ook goed in deze behoefte van de gebruikers voorziet.

E.7.3 Tot slot

Certificeren van modems is een continu proces. Modem/router combinaties worden steeds getest waar diensten en netwerkarchitectuur en implementatie steeds veranderd. Dit proces

moet op een of andere manier ook toegepast worden voor alternatieve modems. Het is maar zeer de vraag of een vrije modem leverancier (vendor) zich wil houden aan het proces dat nu door VodafoneZiggo wordt gebruikt. De kortste tijd nodig om een modem te testen en te certificeren is minimaal een jaar, maar het is meestal langer.

Het lijkt ook niet in het belang van gebruikers dat apparaten onbruikbaar worden als een vendor de updates niet meer ondersteunt. Je ziet dit nu bij smart Tv's (die ineens Netflix niet meer ondersteunen bijvoorbeeld) en smartphones.

Bij VodafoneZiggo gaan modems gemiddeld 4 jaar mee. In het veld zijn er modems wel 10 jaar staan. Echt oudere modems (bijvoorbeeld nog werkend op Docsis 2.0) worden actief vervangen. Bij overstap naar Docsis 3.1 moet er een actieve slag gemaakt worden om oude apparatuur uit te schakelen en te vervangen door nieuwe apparatuur, om het netwerk als geheel zo efficiënt mogelijk te houden.

E.7.a. Bijlage bij interviewverslag VodafoneZiggo

Zie apart bijgevoegde pdf, door Stratix per mail ontvangen op 17-8-2018.

E.8 Interviewverslag VTKE, Verbund der Telekommunikations-Endgerätehersteller

Interview regarding the concept report "Beleidsonderzoek modemkeuze - Analyse consultatiereacties betreffende technische implicaties vrije modemkeuze"

Time: Tuesday 28 august 2018, 11:00h.
Location: Hilversum (conference call)
Participants: Natascha Linssen (lawyer, Dirkzwager)
Jan Buis (Vice President Wireless LAN, IoT & Switches, Lancom)
Dieter Fischer (TAS)
Dr. Gerd Thiedemann (Head of Product Management, AVM)
Eric van Uden (Country Manager NL, AVM)
Benedikt Großmann (Public Affairs Manager, AVM)
David Yoshikawa (senior consultant, Stratix)
Sietse van der Gaast (senior consultant, Stratix)
Hind Abdulaziz (consultant, Stratix)

E.8.1 General impression of the draft report

Basically the overall impression that VTKE has of the report is good. The general thoughts of the report are recognized and acknowledged by the VTKE. Most important for VTKE is the freedom to choose telecom equipment that is attached to the network termination point, terminated in a passive kind of socket.

One missing point of detail could be that IPTV needs some more discussion, as the proposed legislation and its interpretation may in the current form be very difficult to achieve.

E.8.2 Specific topics and issues

A number of specific issues were discussed:

1. Opening up the 'set top boxes' probably adds too much complexity
2. This legislation fits in a long historical trend towards customer freedom
3. Promote or mandate 'best practices' implementation consultation groups
4. The need to prohibit strategic product designs
5. Stress the need to be able to get all necessary information, including credentials
6. Announcement of similar legislation in Italy
7. Regulation of re-imbursement if operator equipment is not used

In the next paragraphs a summary is given of the discussions on each of these topics.

E.8.2.1 Opening up the 'set top boxes' probably adds too much complexity

The now proposed legislation seems to aim at establishing an 'open setup box'. According to VTKE this particular goal will probably be very difficult to achieve because content providers demand specific products with specific encryption and DRM functionalities. However, VTKE is in favour of opening up the general (IP) interface between modem/router and STB, but not necessarily mandate detailing on a service level.

So although it is important that consumers can choose telecom terminal equipment such as modems, routers, etc, VTKE argues that a STB is not similar to telecom terminal equipment, as a STB needs something (a connection) in between.

According to VTKE's view and based on the Directive 2008/63/EC, Terminal equipment is connected directly and indirectly to the last mile of the telecommunication network and for this kind of equipment it should be possible for consumers to choose alternatives if desired.

VTKE believes a public network operator (PNO) should be obliged to specify and publish all interfaces that are related to all services under control of the PNO, such as internet access, telephony, etc., but not necessarily to all kinds of services that are delivered over the top (over the internet) such as Netflix, etc.

E.8.2.2 This legislation fits in a long historic trend towards customer freedom

According to VTKE the proposed legislation must be seen in a historic context. The principle of freedom of choice was set up already around 20 years ago. In many countries freedom of choice of DSL modems (and to a certain degree also cable modems) by customers was already in place. At some point however network operators started to build and promote a situation in which only their equipment could be used. This gradually led to the development and deployment of 'operator owned' IP home platforms for the provision of TV, phone services and the internet access with limited flexibility towards customers.

From 2001, in Germany ITU regulation, based on the European regulation (R&TTE Directive 1999/5/EC) was adopted. So xDSL (80% of broadband networks in Germany is xDSL) was already open. VTKE estimates 40% to 30% of DSL CPE to be bought in retail stores. Cable internet was rolled out slowly starting in 2006 and was initially not targeted as a telco service under EU regulation. It was late to open up for user terminals (2nd half of 2016 due to new legislation) Today cable makes 20% of broadband networks in Germany. But for instance in the USA the cable network was always open. And since 2016 there has been a significant uptake in the sales of modem routers in Germany. In 2017, the number of cable CPE sold in the German retail market contributed to around 20% of the 2017 increase in end users using cable. In addition, there is a significant growth rate for retail cable modems.

According to VTKE there are no publicly available figures or data regarding router sales since the law came into force in August 2016 that refer only to one access technology (cable). However, the article below shows the doubling of households with their own routers in 2018 compared to 2017 at Unitymedia and Vodafone.

Telecompaper.com, 29th August 2018: Unitymedia states that the households that use their own router equipment is doubled (see link: <https://www.telecompaper.com/nieuws/unitymedia-meldt-verdubbeling-van-huishoudens-met-eigen-router--1258420>)

E.8.2.3 Promote or mandate 'best practices' implementation consultation groups

Undertakings in other countries (like in Germany, UK and Switzerland) lead to groups with delegates of operators and manufacturers to come to best practices what is necessary to provide devices and deliver services for network operators. Also the ETSI played an important role in that.

E.8.2.4 The need to prohibit strategic product designs

A point that is missing in the report but has been mentioned in the consultation reaction from VTKE is that VTKE foresees that (V)DSL and cable operators may not be keen to provide all information necessary to connect any kind of modem, and particularly that they may try to design their modems and routers in such way that it would be virtually impossible to use other equipment than the equipment provided by the service provider.

VTKE thinks that it should be explicitly prohibited to strategically design products in such a way that it can refer to exceptions in the legislation or otherwise limit the freedom of choice that can be given to end customers.

E.8.2.5 Stress the need to be able to get all necessary information, including credentials

VTKE thinks that in the current draft legislation the proposal that all information necessary to build devices and deliver services must be made more specific. In the opinion of VTKE now there is room for interpretation for network operators, and this may lead to manufactures and customers not be able to receive the proper information needed to build, install and configure alternative equipment.

For instance, it should be mandatory for network operators to provide customers with the necessary credentials such as logins and passwords that are used for the services that the customer is subscribed to. This is explicitly written in the German version of this legislation but does not seem to be explicitly put in the Dutch version.

E.8.2.6 Announcement of similar legislation in Italy

Very recently also the Italian regulator announced regulation that will improve the freedom of modem choice in Italy.

A non-official translation of the proposed legislation in Italy was sent by Natascha Linssen to EZK for information. VTKE thinks that this proposal has some valid arguments concerning the specifications of the NTU and the necessary information exchange between device manufacturers and network providers.

E.8.2.7 Regulation of re-imbursement if operator equipment is not used

Another observation of VTKE that was not yet mentioned in the consultation response is that there are 'hidden costs' for customers in the modems and other equipment provided by the operators. Freedom of choice should also mean freedom not to receive the standard equipment, in other words customers should be able to get reimbursement when they do not use the equipment that was provided to them by the network operator.

There is currently no regulation in force that allows customers to get reimbursement from network operators in such cases, but this would be a logical next step. In Germany in the business market already in general the customer has the choice which modem to use and in that case no modem is provided – and billed – by the service provider.

E.8.3 Concluding thoughts

According to VTKE the proposed regulation confirms the freedom of choice of terminal equipment. Most important for the VTKE is that the NTU is specified in a correct way, that freedom of choice for end user equipment is guaranteed and that competition is improved.

Stratix

Stratix B.V.

Villa Hestia - Utrechtseweg 29
1213 TK Hilversum

Telefoon:	+31.35.622 2020
E-mail:	office@stratix.nl
URL:	http://www.stratix.nl
Reg. no.:	57689326
IBAN:	NL85ABNA0513733922
BIC:	ABNANL2A
VAT:	NL8526.92.079.B.01