



Forum Standaardisatie

Expertadvies IPv6

Datum 9 augustus 2010

Colofon

Projectnaam	Expertadvies IPv6
Versienummer	1.01 (definitief)
Locatie	
Organisatie	Forum Standaardisatie Postbus 84011 2508 AA Den Haag forumstandaardisatie@logius.nl
Auteurs	dr. ir. H. Eertink ir. Michael van Bekkum

Inhoud

Colofon	2
Inhoud	3
Managementsamenvatting	5
1 Doelstelling expertadvies	7
1.1 <i>Achtergrond</i>	7
1.2 <i>Proces</i>	7
1.3 <i>Vervolg</i>	8
1.4 <i>Samenstelling expertgroep</i>	8
1.5 <i>Toelichting IPv6</i>	9
1.6 <i>Relatie met andere open/gangbare standaarden</i>	10
1.7 <i>Leeswijzer</i>	11
2 Toepassings- en werkingsgebied	12
2.1 <i>Functioneel toepassingsgebied</i>	12
2.2 <i>Organisatorisch werkingsgebied</i>	13
3 Toetsing van standaard aan criteria	14
3.1 <i>Openheid</i>	14
3.1.1 <i>Goedkeuring en handhaving</i>	14
3.1.2 <i>Beschikbaarheid</i>	14
3.1.3 <i>Intellectueel eigendom</i>	15
3.1.4 <i>Hergebruik</i>	15
3.2 <i>Bruikbaarheid</i>	16
3.2.1 <i>Volwassenheid</i>	16
3.2.2 <i>Functionaliteit</i>	18
3.2.3 <i>Standaarden</i>	18
3.3 <i>Potentieel</i>	18
3.3.1 <i>Leveranciersonafhankelijkheid</i>	18
3.3.2 <i>Interoperabiliteit</i>	19
3.4 <i>Impact</i>	19
3.4.1 <i>Bedrijfsvoering</i>	19
3.4.2 <i>Informatievoorziening</i>	20
3.4.3 <i>Technologische risico's</i>	20
3.4.4 <i>Beveiliging en privacy</i>	21
3.4.5 <i>Migratie</i>	21
4 Business Case	23

5 Advies aan Forum en College	25
5.1 <i>Samenvatting van de toetsingscriteria</i>	25
5.2 <i>Advies</i>	26
6 Referenties	27

Managementsamenvatting

Dit rapport bevat het advies van de expertgroep IPv6 aan het Forum Standaardisatie en het College Standaardisatie over het opnemen van de standaard IPv6 [1], op de lijst met open standaarden, die vallen onder het "pas toe of leg uit"-regime (comply-or-explain).

IPv6 voorziet in een specificatie voor het Internet Protocol, dat communicatie van data over een netwerk van onderling verbonden ICT systemen mogelijk maakt. De IPv6 standaard voorziet daarbij o.a. in oplossingen voor de structuur en opbouw van de data en de adressering die noodzakelijk is om de data tussen ICT systemen te kunnen uitwisselen.

IPv6 is de beoogde opvolger van IPv4, de huidige defacto standaard op dit gebied. IPv6 biedt daarbij geen backwards compatibiliteit met IPv4¹ en zal dus niet een directe vervanger zijn van IPv4: beide standaarden zullen geruime tijd naast elkaar bestaan.

De expertgroep is tot de conclusie gekomen dat IPv6 opgenomen kan worden op de lijst met open standaarden.

Belangrijkste punten uit dit advies zijn:

- De standaard IPv6 voldoet aan de gestelde criteria met betrekking tot openheid, bruikbaarheid, potentieel en impact.
- De expertgroep adviseert om het organisatorisch werkingsgebied van IPv6 overeen te laten komen met het werkingsgebied, waarop het "pas toe of leg uit" principe van toepassing is, te weten: overheden (Rijk, provincies, gemeenten en waterschappen) en instellingen uit de (semi-) publieke sector².
- Als functioneel toepassingsgebied adviseert de expertgroep "*communicatie op netwerkniveau tussen alle organisaties, individuele eindgebruikers, apparaten, diensten en sensoren*".
- IPv6 draagt bij aan verbeterde interoperabiliteit: er zijn nu interoperabiliteitsproblemen aan te wijzen tussen overheidspartijen onderling, die door inzet van IPv6 opgelost kunnen worden. Daarbij geldt dat het in alle gevallen raadzaam is om voorlopig naast IPv6 ook de nu gangbare versie IPv4 te (blijven) ondersteunen ("dual stack"). Er is geen impact op de leveranciers-onafhankelijkheid.
- De invoer van IPv6 is onvermijdelijk gezien het beperkte aantal beschikbare IPv4 adressen en de toename van het aantal apparaten met netwerktoegang. Dan zal er een situatie ontstaan waarin beide technologieën (IPv4 en IPv6) gebruikt worden, waarbij beheerslasten (onderhouden van twee technologieën)

¹ <http://www.isoc.org/isoc/conferences/ipv6panel/docs/20090324-ietf-ipv6-panel.txt>

² Zoals vastgelegd in het actieplan "Nederland Open in Verbinding" [2].

aanvankelijk toe zullen nemen. Het toepassen van IPv6 heeft een belangrijk positief effect op het realiseren van toegankelijkheid en bereikbaarheid van (overheids)diensten, waarmee continuïteit van de bedrijfsvoering ook voor de toekomst wordt gewaarborgd.

- Een geforceerde uitrol moet waar mogelijk worden voorkomen, ten behoeve van een kostenefficiënte uitrol. Het uitstellen van opname van IPv6 op de lijst met open standaarden, zal leiden tot een situatie waar in de komende jaren de kosten om dan alsnog IPv6 in te voeren bovenproportioneel toenemen. Er is geen sprake van een "harde deadline" zoals bij het Millenniumvraagstuk, maar wel van een oplopende kostencurve bij uitstel, omdat dan de invoering niet meer efficiënt in reguliere activiteiten van de lijnorganisaties kunnen plaatsvinden. Zo'n keuze leidt later tot een onevenredig dure inhaalslag.

1 Doelstelling expertadvies

1.1 Achtergrond

De staatssecretaris van Economische Zaken heeft op maandag 17 september 2007 het actieplan open standaarden en open source software aan de Tweede Kamer gestuurd. Het doel van het actieplan is om de informatievoorziening toegankelijker te maken, onafhankelijkheid van ICT-leveranciers te creëren en de weg vrij te maken voor innovatie.

Een onderdeel van het actieplan is het opstellen van een lijst met standaarden, die vallen onder het principe "pas toe of leg uit" (comply-or-explain). Het College Standaardisatie spreekt zich uit over de standaarden die op de lijst zullen worden opgenomen, o.a. op basis van een expertbeoordeling van de standaard.

De experts zijn verzameld in een expertgroep, die de standaard heeft beoordeeld aan de hand van een aantal criteria. Deze criteria - en de uitwerking ervan in de vorm van concrete vragen - worden in het hier voorliggende expertadvies genoemd en behandeld. De criteria en procedure zijn overgenomen uit het rapport "Open standaarden: het proces om te komen tot een lijst met open standaarden", geaccordeerd door het College Standaardisatie en te vinden op de website van het Forum Standaardisatie [3].

IPv6 is aangemeld voor opname op de lijst met open standaarden voor "pas toe of leg uit" door SURFnet. De opdracht aan de expertgroep was om een advies op te stellen over het wel of niet opnemen van IPv6 op de lijst met open standaarden, al dan niet onder bepaalde voorwaarden. Daarbij heeft de expertgroep, nadrukkelijk gekeken naar de samenhang tussen IPv6 en de huidige, zeer gangbare voorloper IPv4. Bovendien heeft de expertgroep gekeken naar de Business Case.

1.2 Proces

Voor het opstellen van dit advies is de volgende procedure doorlopen:

- De expertgroep is begonnen met het individueel scoren van IPv6 op basis van een vragenlijst. Deze vragenlijst bevat de criteria zoals beschreven in het hierboven genoemde rapport. Op basis van de verkregen antwoorden hebben voorzitter en begeleider van de expertgroep de verschillende knelpunten geïdentificeerd.
- Vervolgens is de expertgroep op 22 juli 2010 bijeengekomen om de bevindingen in het algemeen en de geïdentificeerde knelpunten in het bijzonder te bespreken. Tijdens deze bijeenkomst zijn ook het toepassings- en werkingsgebied vastgesteld.

De uitkomsten van de expertgroep zijn door de voorzitter en begeleider verwerkt in dit advies rapport. Een eerste conceptversie is aan de leden van de expertgroep gestuurd met verzoek om reactie. Nadat de ontvangen reacties zijn verwerkt, zal het rapport worden afgerond en ingediend voor de publieke consultatieronde.

1.3 Vervolg

Het expertadvies zoals in dit document tot stand is gekomen, zal ten behoeve van een publieke consultatie openbaar worden gemaakt door het Bureau Forum Standaardisatie. Alle belanghebbenden kunnen gedurende de consultatieperiode van 5 weken op dit expertadvies reactie geven. Het Bureau Forum Standaardisatie legt vervolgens de reacties voor aan de voorzitter en indien nodig aan de expertgroep.

Het Forum Standaardisatie zal op basis van het expertadvies en relevante inzichten uit de openbare consultatie een advies aan het College Standaardisatie opstellen. Het College Standaardisatie bepaalt uiteindelijk op basis van het advies van het Forum of de standaard op de lijst met gangbare open standaarden of de 'pas toe of leg uit'-lijst komt.

1.4 Samenstelling expertgroep

Voor de expertgroep zijn personen uitgenodigd die vanuit hun persoonlijke expertise of werkzaamheden bij een bepaalde organisatie direct of indirect betrokken zijn bij de standaard. Daarnaast is een onafhankelijke voorzitter aangesteld om de expertgroep te leiden en als verantwoordelijke op te treden voor het uiteindelijke expertadvies.

Als voorzitter is opgetreden dhr. Henk Eertink. Hij is fellow bij Novay en manager van de groep Human Centric services. Bij Novay is hij verantwoordelijk voor de kennisontwikkeling en –exploitatie op het gebied van ubiquitous computing. Hij is actief met Internet technologieën sinds 1989, en met IPv6 sinds begin deze eeuw (onder meer in het EU 6NET project waarin een eerste grootschalige implementatie van IPv6 in Europa is gerealiseerd).

De expertgroep is in opdracht van Forum Standaardisatie begeleid door dhr. Michael van Bekkum, consultant bij TNO Informatie- en Communicatietechnologie.

Aan de expertgroep hebben deelgenomen:

- Dhr. Cees van der Poel (Logius, Diginetwerk)
- Dhr. Michel Voorsluijs (Belastingdienst)
- Dhr. Olaf Kolkman (IAB / NLnetLabs)
- Dhr. Arjen Holtzer (TNO)
- Dhr. Ronald Boon (Rabobank)
- Dhr. Eduard Metz (KPN)
- Dhr. Marco Hogewoning (XS4all)
- Dhr. Hendrik Rood (Stratix)
- Dhr. Rogier Spoor (Surfnet)
- Dhr. Chris Karreman (vtsPN)
- Dhr. Peter Hartman (NiVo)
- Dhr. Andre Engeringh (Randstad)
- Dhr. Maarten Botterman (GNKS Consult)

Om agendatechnische reden kon niet aanwezig zijn:

- Dhr. Hans de Raad (Ministerie van BZK)

1.5 Toelichting IPv6

Dit advies betreft de internet standaard IPv6. De standaard IPv6 kan worden beschouwd als een verzamelnaam voor een aantal samenhangende standaarden, die zijn vastgelegd in zogenaamde RFC's³. Onderstaande verzameling van RFC's is door de expertgroep beoordeeld:

Hoofd RFC

RFC 2460 Internet Protocol, Version 6 (IPv6) Specification

Essentiële core RFC's

RFC 1981 Path MTU Discovery for IP version 6

RFC 4443 Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification

RFC 4861 Neighbor Discovery for IP version 6 (IPv6)

RFC 4862 IPv6 Stateless Address Autoconfiguration

RFC 4291 IP Version 6 Addressing Architecture

Relatie tussen node, services en andere RFC's

RFC 4294 IPv6 Node Requirements

Transitie Mechanismen

RFC 4213 Basic Transition Mechanisms for IPv6 Hosts and Routers

Bovenstaande RFC's zijn niet alle RFC's die betrekking hebben op IPv6. De bovenstaande lijst vertegenwoordigt echter die specificaties, die naar de mening van de expertgroep een noodzakelijke voorwaarde zijn om IPv6 in de praktijk succesvol te kunnen inzetten en gebruiken. De kern van de IPv6 standaard is daarbij gespecificeerd in RFC 2460⁴. De overige standaarden specificeren

- essentiële RFCs die altijd geïmplementeerd moeten worden om de kernfunctionaliteit van het Internet Protocol te realiseren (RFC's 1981,4443, 4861, 4862, 4291)
- de eisen die gesteld worden aan IPv6 nodes (RFC4294). Dit document specificeert welke van de essentiële RFC's verplicht geïmplementeerd moeten worden voor (netwerk)componenten en eindsystemen.
- de transitie van IPv4 naar IPv6 en mechanismen om co-existentie en compatibiliteit met IPv4 te bewerkstelligen (RFC 4213).

De IPv6 standaard wordt beheerd en onderhouden door de Internet Engineering Task Force (IETF)⁵, een orgaan dat Internet standaarden ontwikkelt en daarbij nauw samenwerkt met o.a. W3C. Werk aan versie 6 van het Internet Protocol (IPv6) is gestart in 1994. De huidige specificatie RFC 2460 is gepubliceerd in 1998.

IPv6 voorziet in een specificatie voor het Internet Protocol, dat communicatie van data over een netwerk van onderling verbonden ICT systemen mogelijk maakt. De IPv6 standaard voorziet daarbij o.a. in

³ Request for Comments, het standaard publicatieformaat voor de Internet Standaarden van de IETF (<http://tools.ietf.org/html/rfc2026>).

⁴ <http://tools.ietf.org/html/rfc2460>

⁵ <http://www.ietf.org/>

oplossingen voor de structuur en opbouw van de data en de adressering die noodzakelijk is om de data tussen ICT systemen te kunnen uitwisselen.

De belangrijkste motivatie voor het werk aan IPv6 was het voorziene gebrek aan IPv4 adressen⁶. Door slimme uitgifte van adressen en door op een slimme manier met de beperkte adresruimte om te gaan⁷, is de noodzaak om IPv6 in te voeren vertraagd. Op dit moment is het restant aan adressen echter zo beperkt, dat interoperabiliteit tussen systemen op relatief korte termijn (+/- 2 jaar) in grote delen van de wereld niet meer gegarandeerd kan worden⁸: delen van het internet (in zowel binnenland als buitenland) zullen door het tekort IPv6-only worden. Als overheidsorganisaties alleen IPv4 gebruiken zullen diensten van de overheid niet meer voor deze IPv6-only partijen bereikbaar zijn. Omgekeerd kan de overheidsorganisaties dan geen gebruik meer maken van de ICT diensten die deze IPv6-only organisaties leveren.

IPv6 lost dit probleem op door o.a. een (veel) grotere adresruimte te bieden⁹. Aangezien de standaard IPv6 ook een volledige herziening van het Internet Protocol betreft, is parallel ook gewerkt aan eenvoudiger beheer, en betere ondersteuning van beveiliging¹⁰.

1.6 Relatie met andere open/gangbare standaarden

IPv6 is ontwikkeld als de natuurlijke opvolger van het huidige Internet Protocol IPv4. Zowel IPv4 als IPv6 staan op dit moment op de lijst met gangbare standaarden. IPv6 is aangemeld om opgenomen te worden op de lijst met open standaarden voor "pas toe of leg uit" om gebruik van de standaard en interoperabiliteit verder te bevorderen.

Beide standaarden kunnen, zullen en moeten naar de mening van de expertgroep naast elkaar binnen hetzelfde netwerk gebruikt worden. In dit expertadvies zal uitgebreid worden ingegaan op de wijze waarop beide standaarden naast elkaar gebruikt kunnen worden.

IPv6 kent ook een relatie met de volgende standaarden die voorkomen op de lijst met gangbare standaarden:

- Domain Name System (DNS)
- Dynamic Host Configuration Protocol (DHCP)
- Security Architecture for the Internet Protocol (IPsec)

⁶ De IPv4 adresruimte bedraagt 32 bits, dwz. ongeveer 4 miljard adressen. Ter vergelijking: dit is nu al minder dan het aantal telefoons dat op de wereld in gebruik is.

⁷ O.a. door gebruik van Network Address Translation (NAT) en lokaal geldige adressen, zie IETF RFC1631 en RFC3022, <http://tools.ietf.org/html/rfc3022> en <http://tools.ietf.org/html/rfc3022>

⁸ http://www.computable.nl/artikel/ict_topics/internet/3436317/1282763/ipv4voorraad-raakt-binnen-een-jaar-op.html

⁹ IPv4 gebruikt 32 bits (ongeveer 4.3×10^9) adressen, waar IPv6 gebruik maakt van 128 bits (ongeveer 3.4×10^{38}) adressen.

¹⁰ Door de protocol beveiliging, vastgelegd door IPSEC, als integraal onderdeel mee te nemen in het ontwerp.

1.7 Leeswijzer

In hoofdstuk 2 wordt beschreven in welke gevallen IPv6 functioneel gezien gebruikt moet worden (functioneel toepassingsgebied) en door welke organisaties IPv6 gebruikt zou moeten worden (organisatorisch werkingsgebied). Om te bepalen of IPv6 opgenomen moet worden op de lijst met open standaarden is deze getoetst aan een viertal door het College Standaardisatie vastgestelde criteria. In hoofdstuk 3 staat het resultaat van deze toetsing. Hoofdstuk 4 bevat een samenvatting van de toetsresultaten op hoofdlijnen en het advies van de expertgroep aan het forum.

2 Toepassings- en werkingsgebied

Van overheidsorganisaties wordt verwacht dat zij de lijst met open standaarden hanteren bij aanbestedingstrajecten volgens het "pas toe of leg uit"-regime. Afhankelijk van de aan te schaffen functionaliteit zal bepaald moeten worden welke koppelvlakken geïmplementeerd moeten worden, en welke standaarden uit de lijst hiervoor ingezet dienen te worden. Om dit te kunnen doen heeft de expertgroep gekeken in welke gevallen IPv6 functioneel gezien gebruik moet worden (functioneel toepassingsgebied), en door welke organisaties IPv6 gebruikt zou moeten worden (organisatorisch werkingsgebied).

2.1 Functioneel toepassingsgebied

De expertgroep heeft zich gebogen over het toepassingsgebied voor IPv6 en heeft daarbij een aantal kenmerken en uitgangspunten vastgesteld met betrekking tot IPv6:

- Het Internet Protocol wordt toegepast om connectiviteit op netwerkniveau te realiseren tussen eind-systemen.
- IPv6 lost een aantal bestaande problemen op. Met name maakt de toepassing van IPv6 het mogelijk om miljarden apparaten *per wereldburger* uniek te adresseren en globaal bereikbaar te maken (door transparante communicatie).

IPv6 moet toegepast worden:

- Voor het realiseren van toegankelijkheid en bereikbaarheid van (overheids)diensten, ook voor organisaties en individuen die alleen via IPv6 bereikbaar zijn.
- Voor de communicatie tussen de eindsystemen van (overheids)diensten onderling, waarbij de communicatie over organisatiegrenzen plaatsvindt.
- Het gebruik van IPv6 wordt daarmee vooral een vereiste op het koppelvlak van de organisatie, aan de "buitenkant".
- om voorbereid te zijn op toekomstige uitwisseling van data tussen allerhande apparaten. De grootschalige introductie van sensoren in ondermeer mobiliteitsvraagstukken¹¹, bij dijkbewaking en in slimme energiemeters moet immers mogelijk zijn voor miljoenen gebruikers in Nederland.

De expertgroep heeft zich ook gebogen over de verhouding tussen IPv4 en IPv6. Dit is vooral van belang omdat IPv4 de huidige defacto standaard voor uitwisseling van data is voor overheden, bedrijven en consumenten en IPv6 geen backwards compatibiliteit biedt met IPv4¹². Er moet dus goed worden vastgesteld wat ingebruikname van IPv6 betekent voor het gebruik van IPv4 in huidige en toekomstige ICT systemen en toepassingen.

De expertgroep verwacht hierbij dat gedurende een lange periode (10-20 jaar) IPv4 en IPv6 tegelijkertijd gebruikt gaan worden binnen één netwerk. De IETF heeft dan ook veel aandacht geschonken aan de problemen bij co-existentie van beide standaarden. In RFC 4213 zijn

¹¹ "Anders betalen voor mobiliteit", <http://www.rijksoverheid.nl/onderwerpen/kilometerprijs/>
¹² <http://www.isoc.org/isoc/conferences/ipv6panel/docs/20090324-ietf-ipv6-panel.txt>

oplossingen uitgewerkt voor transitie van IPv4 naar IPv6 en voor het gebruik van zowel IPv4 als IPv6 op één systeem¹³. Bij het vaststellen van de relevante RFC's voor beoordeling van IPv6 voor opname op de lijst met open standaarden, is deze RFC door de expertgroep dan ook als een van de vereiste onderdelen van de IPv6 standaard meegenomen.

Het toepassingsgebied van IPv6 is sterk overlappend aan dat van IPv4. De schaalbaarheid van IPv4 is echter zodanig beperkt dat de transparantie van het Internet en daarmee mogelijkheden voor innovatie op middellange termijn in gevaar komen. IPv6 borgt de open architectuur voor de verdere evolutie van het Internet. Die open architectuur en blijvende beschikbaarheid van adressen zorgen er op de lange duur voor dat innovatie en groei op het Internet mogelijk blijft¹⁴.

Als functioneel toepassingsgebied adviseert de expertgroep daarom

"communicatie op netwerkniveau tussen alle organisaties, individuele eindgebruikers, apparaten, diensten en sensoren"

Communicatie tussen alle partijen en systemen wordt mogelijk, doordat IPv6 het mogelijk maakt ieder apparaat van een unieke (adres)identificatie te voorzien in een netwerk van wereldwijde omvang.

2.2 Organisatorisch werkingsgebied

De expertgroep adviseert om het organisatorisch werkingsgebied van IPv6 overeen te laten komen met het werkingsgebied, waarop het "pas toe of leg uit" principe van toepassing is, te weten: overheden (Rijk, provincies, gemeenten en waterschappen) en instellingen uit de (semi-) publieke sector¹⁵.

Bovenstaande omschrijving van het werkingsgebied bevat naar de mening van de expertgroep direct of indirect alle relevante partijen op wie de standaard van toepassing is. De expertgroep zag dan ook geen reden om bovenstaand werkingsgebied verder in te perken.

¹³ In IETF RFC 4213 worden twee mechanismen gespecificeerd: 'dual stack' en 'configured tunneling'. Dual stack 'gaat uit van complete implementatie van beide protocollen (IPv4 en IPv6). Configured Tunneling voorziet in een manier om IPv6 packets via een ongewijzigde IPv4 infrastructuur te vervoeren, <http://tools.ietf.org/html/rfc4213>

¹⁴ <http://www.ripe.net/news/community-statement.html>

¹⁵ Zoals vastgelegd in het actieplan "Nederland Open in Verbinding" [3].

3 Toetsing van standaard aan criteria

Om te bepalen of IPv6 opgenomen moet worden op de lijst met open standaarden is deze getoetst aan een aantal criteria. Deze criteria staan beschreven in het rapport, "*Open standaarden, het proces om te komen tot een lijst met open standaarden*" [3] en staan op de website www.open-standaarden.nl. Het resultaat van de toetsing zal in dit hoofdstuk per criterium beschreven worden. Voor de volledigheid is tevens de definitie van elk criterium opgenomen (*cursief*).

3.1 Openheid

3.1.1 *Goedkeuring en handhaving*

De standaard is goedgekeurd en zal worden gehandhaafd door een non-profit organisatie. De lopende ontwikkeling gebeurt op basis van een open besluitvormingsprocedure die toegankelijk is voor alle belanghebbende partijen (consensus of meerderheidsbeschikking enz.).

IPv6 is in beheer bij IETF. De verdere ontwikkeling en het onderhoud van IPv6 wordt vormgegeven door de reguliere standaardisatieproces van IETF, zoals vastgelegd in RFC 2026¹⁶. Aan dit standaardisatieproces kan iedereen (incl. ieder individu) deelnemen, hetzij via meetings, hetzij via mailing lists. De IETF kent geen formeel lidmaatschap of lidmaatschapseisen. Het standaardisatieproces maakt gebruik van een besluitvormingsprocedure via het principe van "rough consensus"¹⁷, waarbij de dominante mening van een groep, zoals door de voorzitter vastgesteld, de basis voor een beslissing vormt. Documenten, mailing lijsten en verslagen van bijeenkomsten en besluiten zijn publiekelijk beschikbaar op het internet. De IETF is een onderneming zonder winstoogmerk.

Hiermee is naar de mening van de expertgroep voldaan aan dit criterium.

3.1.2 *Beschikbaarheid*

De standaard is gepubliceerd en over het specificatiedocument van de standaard kan vrijelijk worden beschikt of het is te verkrijgen tegen een nominale bijdrage. Het moet voor een ieder mogelijk zijn om het te kopiëren, beschikbaar te stellen en te gebruiken om niet of tegen een nominale prijs.

Alle IETF standaarden zijn vrij en kosteloos beschikbaar op het Internet , via <http://www.ietf.org/>.

¹⁶ The Internet Standards Process -- Revision 3, <http://tools.ietf.org/html/rfc2026>

¹⁷ IETF Working Group Guidelines and Procedures, <http://tools.ietf.org/html/rfc2418>

3.1.3 *Intellectueel eigendom*

Het intellectuele eigendom – met betrekking tot mogelijk aanwezige patenten – van (delen) van de standaard is onherroepelijk ter beschikking gesteld op een "royalty-free" basis.

De Intellectual Property Rights (IPR) policy van IETF is vastgelegd in RFC 3979¹⁸. Daarin is vastgelegd dat leden van de werkgroep van een specifieke standaard, bestaande IPR moet onthullen, die in de ogen van de werkgroep relevant is voor de standaard die in deze werkgroep in behandeling is. Partijen die hebben meegewerkt aan de IPv6 standaard hebben verklaard dat zij *geen* IPR rechten claimen.

IPR claims worden vastgelegd in de RFC van de betreffende standaard en kunnen op de website van IETF worden nagegaan, door gebruik te maken van een IPR zoekfunctie¹⁹. Dit betekent echter niet dat er garanties gegeven kunnen worden over eventuele *toekomstige claims* met betrekking tot het intellectueel eigendom. Voor alle RFC's die in dit advies met betrekking tot IPv6 worden beoordeeld geldt echter dat er sinds de start van het standaardisatieproces begin jaren 90 nog geen IPR claims zijn voorgekomen. De expertgroep is daarom van mening dat daarmee in voldoende mate aan dit criterium wordt voldaan.

3.1.4 *Hergebruik*

Er zijn geen beperkingen omtrent het hergebruik van de standaard.

Er worden aan het hergebruik van de standaard zelf geen additionele eisen gesteld.

De copyright policy (auteursrechtenbeleid) van de IETF ten aanzien van IETF documenten waarin de standaard is vastgelegd, is in twee documenten verwoord, te weten RFC 5378²⁰ en de 'IETF Trust's Legal Provisions Relating to IETF Documents'²¹. Hierin is ondermeer vastgelegd, dat:

- Elk document van de IETF vrijelijk mag worden gekopieerd, gepubliceerd, getoond, vertaald en gedistribueerd.
- Elk document van de IETF alleen mag worden gemodificeerd en mag worden gebruikt voor afgeleide producten binnen het IETF standaardisatieproces.
- Iedereen ongewijzigde IETF documenten mag publiceren en vertalen voor elk doeleinde, ook buiten het standaardisatieproces.
- Het niet is toegestaan om aanpassingen te doen aan en afgeleide producten te maken (behalve vertalingen) van IETF documenten en bijdragen buiten het standaardisatieproces. Na consultatie van de gemeenschap kunnen dergelijke rechten per geval eventueel worden toegekend.

Op basis van bovenstaande is de expertgroep van mening dat er geen beperkingen zijn omtrent het hergebruik van de standaard.

¹⁸ Intellectual Property Rights in IETF Technology, <http://www.ietf.org/rfc/rfc3979.txt>

¹⁹ IPR Search, <https://datatracker.ietf.org/ipr/search/>

²⁰ <http://www.rfc-editor.org/rfc/rfc5378.txt>

²¹ <http://trustee.ietf.org/docs/IETF-Trust-License-Policy.pdf>

3.2 Bruikbaarheid

3.2.1 Volwassenheid

De standaard is voldoende uitgekristalliseerd.

In het standaardisatieproces van de IETF gaan specificaties door een aantal stadia van volwassenheid heen, die samen ook wel het 'standards track' worden genoemd²². Er zijn drie niveau's van volwassenheid voor een standaard te onderscheiden, te weten (in toenemende mate van volwassenheid):

- 'Proposed standard' : dit is een stabiele specificatie, waarin alle ontwerpkeuzen zijn uitgewerkt, die in het algemeen goed wordt begrepen, die aan significante review is blootgesteld en die algemeen door de gemeenschap als waardevol wordt gezien.
- 'Draft standard' : dit is een specificatie op basis waarvan ten minste twee onafhankelijke en interoperabele implementaties zijn ontwikkeld, op basis van verschillende broncode en waarmee met succes voldoende praktijkervaring is opgedaan.
- 'Internet standard' : een specificatie waarmee in de praktijk ervaring is opgedaan in een significante hoeveelheid implementaties, kan tot Internet Standard worden verheven. Deze standaard kent dan een hoge graad van technische volwassenheid.

De huidige status van een RFC in het standaardisatieproces en de updates die op de RFC hebben plaatsgevonden, zijn in te zien op de website van de IETF²³. In *Tabel 1* is van elk van de RFC's, die wordt beoordeeld in het kader van dit expertadvies, de status weergegeven.

RFC	Titel	Status	Datum
2460	Internet Protocol, Version 6 (IPv6) Specification	Draft	Dec. 1998
1981	Path MTU Discovery for IP version 6	Draft	Aug. 1996
4443	Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification	Draft	Mrt. 2006
4861	Neighbor Discovery for IP version 6 (IPv6)	Draft	Sept. 2007
4862	IPv6 Stateless Address Autoconfiguration	Draft	Sept. 2007
4291	IP Version 6 Addressing Architecture	Draft	Feb. 2006
4294	IPv6 Node Requirements	Informational	Apr. 2006
4213	Basic Transition Mechanisms for IPv6 Hosts and Routers	Proposed	Okt. 2005

Tabel 1 RFC status

In de tabel is te zien dat de alle standaarden de status van 'draft standard' of 'proposed standard' hebben. Deze RFC's zijn in hoge mate stabiel en aan weinig veranderingen onderhevig (sinds 1998 zijn er slechts twee kleine aanpassingen geweest op de overall IPv6 standaard).

De uitzondering is RFC 4294: deze heeft de status 'informational'. Deze RFC voorziet dan ook niet in een specificatie op basis van consensus, maar is informatief en verschaft voor de 'IPv6 node requirements' referenties

²² The internet Standards Process – Revision 3, <http://tools.ietf.org/html/rfc2026>

²³ Via <http://www.rfc-editor.org/>

naar andere relevante RFC's. Deze RFC is aan wijzigingen onderhevig, maar zal op de uitgekristalliseerde functionaliteit van bovenstaande RFC's nauwelijks aanpassingen kennen.

De expertgroep is van mening, dat daarmee de IPv6 standaard als geheel in voldoende mate is uitgekristalliseerd.

De verdere ontwikkeling en het onderhoud van de standaard zijn verzekerd.

Ja, de organisatie die de standaard beheert (IETF) bestaat sinds 1986 en heeft aangetoond dat zij een stabiele organisatie is die over een lange periode in staat is om standaarden te ontwikkelen en beheren. De standaarden die onder IPv6 vallen worden verder ontwikkeld in de diverse werkgroepen van de IETF.

Er is een methode waarmee conformiteit aan de standaard kan worden bepaald.

IPv6 is een 'draft standard' van de IETF. Dat betekent dat interoperabiliteit tussen tenminste twee volledig verschillende software-implementaties van de standaard aangetoond moet zijn. Daarnaast zijn er methodes voor het testen van diverse features (zie <http://ipv6ready.org>). Eventuele interoperabiliteitsgeschillen worden geanalyseerd binnen de IETF en kunnen eventueel leiden tot aanpassingen aan de standaard conform het IETF proces.

Er is voldoende praktijkervaring met het gebruik van de standaard.

Er zijn inmiddels voldoende instellingen en organisaties die IPv6 toepassen zowel commercieel als not-for-profit (Surfnet, universiteiten, SIDN, RIPE NCC, EC). Bij eindgebruikersorganisaties is IPv6 nog relatief onbekend.

Er is nu en in de toekomst voldoende ondersteuning door (meerdere) marktpartijen voor de standaard.

Er zijn productleveranciers (van ondermeer routers, besturingssystemen, etc.) die al jarenlang IPv6 ondersteunen (bijv. Cisco en Juniper, Microsoft, Apple, Linux, etc.). Deze producten zijn zowel in de zakelijke als de consumentenmarkt verkrijgbaar.

In de consumentenmarkt wordt IPv6 nog nauwelijks aangeboden door Internet Service Providers (ISP's). In Nederland is XS4ALL op moment van schrijven van dit rapport de enige aanbieder. In een recente studie is vastgesteld, dat er op dit moment zes ISPs zijn die IPv6 aanbieden op de nederlandse zakelijke markt. Dit zijn: BIT, Breedband Delft, Interoute, Signet, Introweb en Proserve [4].

Op de IPv6 functionaliteiten van producten wordt ondersteuning geleverd door de leveranciers die vergelijkbaar is met de ondersteuning voor IPv4.

De verwachting van het toekomstig gebruik van de standaard is positief.

Het gebruik van IPv6 in de nabije toekomst is onvermijdelijk. Adoptie in Nederland blijft wel achterwege bij andere landen [4].

3.2.2 *Functionaliteit*

De standaard voldoet aan de functionele eisen die aan de werking van de standaard gesteld worden binnen het voorgestelde toepassingsgebied.

Binnen het voorgestelde toepassingsgebied van IPv6 is functionaliteit geselecteerd die momenteel in de praktijk van de standaard volledig ondersteund en al toegepast wordt. Naar de mening van de expertgroep zijn er geen functies uit dit toepassingsgebied die de standaard niet ondersteunt.

3.2.3 *Standaarden*

Zijn er concurrerende standaarden? Zo ja, welke en door wie worden die gebruikt? Wat zijn de voor- en nadelen van deze standaard ten opzichte van concurrerende standaarden?

De expertgroep stelt vast, dat IPv4 momenteel de enige concurrent is. IPv4 is momenteel de de-facto standaard voor uitwisseling van data middels het Internet Protocol. IPv6 is ontworpen als opvolger van IPv4 en zal op termijn uitgroeien tot de de-facto standaard voor end-to-end communicatie op basis van het Internet Protocol.

Het toepassingsgebied van IPv6 is daarbij sterk overlappend met dat van IPv4. IPv6 kent als belangrijkste voordeel ten opzichte van IPv4 de grotere adresruimte: IPv6 heeft grootte van het IP adres verhoogd van 32 bits (ca. 4 miljard adressen) naar 128 bits. Hiermee is IPv6 theoretisch in staat om ieder persoon op aarde (ongeveer 7 miljard) meer dan 5×10^{28} adressen toe te kennen.

Daarnaast zijn andere voordelen ten opzichte van IPv4:

- Vereenvoudigde adrestoekenning aan apparaten en systemen.
- Meer flexibiliteit voor opties en uitbreidingen.
- Uitbreidingen voor veiligheid (authenticatie, integriteit, confidentiality) zijn integraal onderdeel van de standaard.
- Het feit dat NAT niet nodig is om verder groei van het Internet te realiseren: IPv4 kan alleen verder groeien door inzet van NAT, wat de nodige connectiviteitsproblemen met zich mee brengt.

3.3 Potentieel

3.3.1 *Leveranciersafhankelijkheid*

Het opnemen van de standaard op de lijst draagt bij aan het vergroten van de leveranciersafhankelijkheid.

De expertgroep is van mening dat het opnemen van de standaard op de lijst niet bijdraagt aan het vergroten van de leveranciersafhankelijkheid. De huidige de-facto standaard IPv4 is al open en volledig leveranciersafhankelijk. Ten aanzien van zowel leveranciers van IPv6 adressen als leveranciers van IPv6-apparatuur en -software neemt de

leveranciersafhankelijkheid dan ook niet toe (maar ook niet af) door opname van IPv6 op de lijst met open standaarden.

3.3.2 *Interoperabiliteit*

Het opnemen van de standaard op de lijst draagt bij aan het vergroten van de interoperabiliteit.

De expertgroep is van mening dat het opnemen van de standaard op de lijst bijdraagt aan het vergroten van de interoperabiliteit. De expertgroep stelt vast dat er op moment van schrijven van dit rapport al interoperabiliteitsproblemen zijn aan te wijzen tussen overheidspartijen onderling, die door inzet van IPv6 opgelost zouden kunnen worden. Dit wordt in belangrijke mate veroorzaakt door het creëren van end-to-end bereikbaarheid met IPv6, waardoor de efficiency vergroot wordt in vergelijking met IPv4. IPv4 vereist namelijk het gebruik van NAT-systemen (omzetten van private IPv4 adressen naar publieke IPv4 adressen en vice-versa). Het gebruik van NAT leidt tot inefficiënties en tot gebrek aan end-to-end bereikbaarheid op applicatieniveau. Het gebruik van NAT leidt bij een aantal belangrijke protocollen (o.a. SIP, FTP, RFC) dan ook tot problemen²⁴.

De problemen die nu al spelen (resp. ontstaan) tussen overheidspartijen gaan op den duur ook op het Internet in brede zin optreden. Deze problemen worden opgelost door middel van IPv6.

3.4 **Impact**

3.4.1 *Bedrijfsvoering*

Brengt de toepassing van de standaard risico's met zich mee op het gebied van de bedrijfsvoering?

Brengt de toepassing van de standaard positieve effecten met zich mee op het gebied van de bedrijfsvoering?

De risico's zijn naar de mening van de expertgroep beperkt omdat IPv6 naast IPv4 uitgerold zal worden en uitgerold zal blijven. Ook voor partijen die diensten afnemen of aanbieden aan de overheid is de impact beperkt omdat deze diensten zowel via IPv4 als IPv6 bereikbaar zullen zijn indien de servers waarop ze aangeboden worden zowel IPv4 als IPv6 ondersteunen. Alle recente operating systemen ondersteunen verder IPv4 en IPv6 tegelijkertijd op één server of client. Er zijn overigens ook diensten op de markt die alleen via IPv6 ontsloten worden.

De expertgroep stelt vast dat het toepassen van IPv6 een belangrijk positief effect heeft op het continuïteit van toegankelijkheid en bereikbaarheid van (overheids)diensten, zeker gezien het feit dat er in de toekomst organisaties en individuen zijn die alleen via IPv6 bereikbaar zijn. Daarmee wordt de continuïteit van de bedrijfsvoering ook voor de toekomst gewaarborgd.

²⁴ IPv6, GOVCERT.NL whitepaper, <http://www.govcert.nl/download.html?f=159>

Een andere belangrijke positieve ontwikkeling is dat nauwe samenwerking of integratie van organisaties niet wordt geremd door de problemen die nu ontstaan bij de samenvoeging van de interne communicatienetwerken binnen organisaties. De overlap die nu kan bestaan tussen de noodzakelijkerwijs gebruikte private adressenreeksen binnen organisaties zal verdwijnen, omdat het gebruik van private adressen in geval van IPv6 niet meer nodig is.

3.4.2 *Informatievoorziening*

Brengt de toepassing van de standaard risico's met zich mee op het gebied van de informatievoorziening?

Brengt de toepassing van de standaard positieve effecten met zich mee op het gebied van de informatievoorziening?

De expertgroep is van mening dat de standaard geen zwaarwegende risico's op het gebied van de informatievoorziening met zich mee brengt. Met betrekking tot informatievoorziening geldt dat bestaande software niet altijd aangepast kan worden aan het gebruik van IPv6. De expertgroep acht de impact op de informatievoorziening op het niveau van IPv6 echter beperkt, omdat de verwachting is dat gedurende een lange periode (10-20 jaar) IPv4 en IPv6 tegelijkertijd gebruikt gaan worden binnen één netwerk.

3.4.3 *Technologische risico's*

Brengt de toepassing van de standaard technologische risico's met zich mee?

Brengt de toepassing van de standaard positieve technologische effecten met zich mee op het gebied van de informatievoorziening?

Een risico dat de expertgroep onderkent is dat er meer technologie onderhouden zal moeten worden en er dus meer beheersinspanning wordt gevraagd, door het feit dat IPv4 en IPv6 tegelijkertijd gebruikt gaan worden binnen één netwerk. Naast IPv4 en IPv6 technologie, zullen ook verbindende technologieën²⁵ tussen beide protocollen om een extra inspanning vragen, bijvoorbeeld voor transitiedoeleinden.

De expertgroep is van mening dat de standaard verder geen andere risico's met zich meebrengt dan de risico's van de introductie van elke nieuwe technologie.

De expertgroep concludeert dat het verwijderen van NAT-systemen (adresvertaling) uit de netwerken als positief effect optreedt. Deze NAT-systemen leiden tot inefficiënties en gebrek aan end-to-end bereikbaarheid, waardoor er configuratie van applicatie-specifieke oplossingen moet plaatsvinden. Het verwijderen van NAT maakt applicaties mogelijk die nu deels worden gefrustreerd in hun werking.

²⁵ Voorbeelden zijn Tunneling (RFC 4213) en "IPv4-mapped" of "IPv4-compatible" IPv6 adres (RFC 4291)

3.4.4 *Beveiliging en privacy*

Brengt de toepassing van de standaard risico's met zich mee op het gebied van beveiliging of privacy?

Brengt de toepassing van de standaard positieve technologische effecten met zich mee op het gebied van de beveiliging en privacy?

De expertgroep onderkent een aantal aandachtspunten op het gebied van beveiliging en privacy. Er zijn een aantal voor- en nadelen op dit gebied bij de uitrol van IPv6.

Het voordeel dat de expertgroep onderkent, is:

- Op dit moment heeft een aantal besturingssystemen IPv6 al standaard 'aan' staan en in gebruik. Dit netwerkverkeer wordt niet altijd gemonitord door de ICT-afdeling wanneer er een IPv4-only beleid is. Het betrekken van IPv6 in het ICT-beleid van organisaties zal er voor zorgen dat de veiligheids- en beveiligingsproblemen die dit met zich mee brengt (inclusief hacking), zullen worden opgemerkt

De risico's die de expertgroep onderkent zijn:

- Firewall implementaties zullen ook op IPv6 uitgevoerd moeten worden. Verkeerde configuratie kan daarbij tot veiligheidsproblemen leiden.
- Door het wegvallen van NAT worden de adressen van de eindpunten zichtbaar voor het hele Internet. Dat kan privacy-problemen opleveren. IPv6 heeft daar de nodige oplossingen voor, maar die staan niet altijd automatisch aan. Dit zal bij implementatietrajecten onder de aandacht moeten worden gebracht.
- Omdat IPv6 naast IPv4 wordt gebruikt zullen voor beide technologieën beveiligingsmaatregelen moeten worden genomen. Het netwerk- en beveiligingsbeheer neemt dus toe.
- IPv6 vraagt om aanpassingen in netwerkbeheer: door het verwijderen van NAT is de traceerbaarheid groter.

De expertgroep concludeert, dat de beveiligings- en veiligheidsrisico's een aandachtspunt zijn, maar geen zwaarwegende risico's met zich brengen.

3.4.5 *Migratie*

Kan er gemakkelijk naar de standaard worden gemigreerd?

De expertgroep stelt vast, dat er maar één waarschijnlijk migratiescenario voorhanden is: de migratie van IP4-only naar co-existentie van IPv6 en IPv4 in een 'dual stack' situatie. De expertgroep verwacht hierbij dat gedurende een lange periode (10-20 jaar) IPv4 en IPv6 tegelijkertijd gebruikt gaan worden binnen één netwerk. De IETF heeft dan ook veel aandacht geschonken aan de problemen bij co-existentie van beide standaarden. In RFC 4213 zijn oplossingen uitgewerkt voor transitie van IPv4 naar IPv6 en voor het gebruik van zowel IPv4 als IPv6 op één systeem²⁶.

²⁶ In IETF RFC 4213 worden twee mechanismen gespecificeerd: 'dual stack' en 'configured tunneling'. Dual stack 'gaat uit van complete implementatie van beide protocollen (IPv4 en IPv6). Configured Tunneling voorziet in een manier om IPv6 packets via een ongewijzigde IPv4 infrastructuur te vervoeren, <http://tools.ietf.org/html/rfc4213>

De aandachtspunten die de expertgroep bij migratie onderkent, zijn de volgende:

- De uitrol van IPv6 moet structureel worden aangepakt. Niet in een project (met eindige doorlooptijd), maar ingebed in de standaard processen van de organisatie.
- De invoering van IPv6 moet gefaseerd worden uitgevoerd. Bijvoorbeeld bij de vervanging van huidige apparatuur moet men IPv6 als vereiste direct meenemen en daarna zowel IPv4 als IPv6 in gebruik nemen.
- Bij migratie moeten in veel gevallen ook de applicaties getest worden voor conformiteit aan IPv6. Als de migratie onderdeel is van de reguliere vervangingscyclus is dat zonder al teveel extra inspanning mogelijk.
- IPv6 moet onderdeel worden van de netwerk-architectuur in brede zin, en zo ook onderdeel van het standaard beheersproces.

Naar de mening van de expertgroep is het positief dat migratie wereldwijd plaatsvindt. Dat betekent dat er in toenemende mate kennis en gereedschappen beschikbaar zijn/komen die deze overgang kunnen ondersteunen.

In de expertgroep is gediscussieerd over de noodzaak voor migratie. Voor Nederland zijn naar verwachting van de expertgroep binnen 2 tot 4 jaar de IPv4 adressen echt schaars²⁷. De expertgroep concludeert ten aanzien van migratie dan ook dat de configuratie van IPv6 nu meegenomen moet worden in de vervanging of uitrol van actieve netwerkcomponenten en eindsystemen, inclusief de ondersteuning daarvan. Dit is noodzakelijk om de universele toegang tot de diensten te kunnen garanderen zonder onderbreking van de dienstverlening (of een onevenredig dure inhaalslag later).

²⁷ Volgens breed geaccepteerde voorspellingen van senior onderzoeker Geoff Huston zullen Nederlandse organisaties (dus ook overheidsorganisaties) vanaf 2012 geen nieuwe IPv4 adressen meer kunnen krijgen van RIPE NCC [4], <http://www.potaroo.net/>

4 Business Case

De expertgroep heeft zich gebogen over de vraag om kosten en baten van implementatie en ingebruikname van IPv6 in een korte analyse uiteen te zetten.

De expertgroep merkt op dat de setting van een expertsessie onvoldoende is om nauwkeurig antwoord te geven op deze vraag. In plaats daarvan heeft de expertgroep de belangrijkste kostenposten en baten op een rij gezet en getracht deze te classificeren naar belangrijkheid en consequenties in termen van middelen (financieel, tijd). Een kwantitatieve schatting van de kosten is daarbij alleen op macroniveau gemaakt.

Als kostenposten onderkent de expertgroep in toenemende mate van vereiste middelen:

- ISP kosten: kosten om IPv6 connectiviteit af te nemen van de huidige provider of om te switchen naar een ISP die IPv6 ondersteunt.
- Kosten routers, netwerkkapparatuur: het vervangen van apparatuur die geen IPv6 ondersteunt.
- Testen van netwerk en applicaties: bestaande hardware- en softwaresystemen zullen grondig moeten worden getest op geschiktheid voor IPv6 en indien nodig moeten worden aangepast of vervangen.
- Opleiding IT medewerkers en staf: de introductie van IPv6 brengt nieuwe mogelijkheden met zich mee en vereist dus nieuwe kennis voor configuratie en beheer.

Enigszins vergelijkbaar grootschalige ICT operaties in het verleden in Nederland (zoals omnummering van het telefoonnetwerk) hebben uitgewezen dat het niet ondenkbaar is dat kosten voor een overstap op IPv6 honderden miljoenen zal bedragen voor de overheid²⁸. De expertgroep is van mening dat een geforceerde uitrol waar mogelijk moet worden voorkomen, ten behoeve van een kostenefficiënte uitrol. Daarom moet men bijtijds (nu al) moet beginnen met de uitrol van IPv6: dit levert op termijn minder kosten op en maakt het mogelijk een geleidelijk migratietraject te doorlopen. Door IPv6 bij vervanging van apparatuur uit te rollen wordt voorkomen dat een transitie in een keer moet plaatsvinden.

Het uitstellen van opname van IPv6 op de lijst met open standaarden, zal leiden tot een situatie waar in de komende jaren de kosten om dan alsnog IPv6 in te voeren bovenproportioneel toenemen. Er is geen sprake van een "harde deadline" zoals bij het Millenniumvraagstuk, maar wel van een oplopende kostencurve bij uitstel, omdat dan de invoering niet meer efficiënt in reguliere activiteiten van de lijnorganisaties kunnen plaatsvinden. Zo'n keuze leidt later tot een onevenredig dure inhaalslag.

De baten die de expertgroep onderkent bij introductie van IPv6 zijn:

- Het realiseren van toegankelijkheid en bereikbaarheid van (overheids)diensten, ook voor organisaties en individuen die (in de toekomst) alleen via IPv6 bereikbaar zijn. Toekomstige

²⁸ De expertgroep geeft in een grove schatting aan dat dit bedrag 10 tot 20% zal zijn van een overstap voor alle organisaties in Nederland, een operatie die zeer waarschijnlijk miljarden kost.

gebruikersgroepen die door het adrestekort van IPv4 op IPv6 zijn aangewezen worden zo niet uitgesloten van overheidsdiensten. Daarmee wordt de continuïteit van de bedrijfsvoering ook voor de toekomst gewaarborgd.

- Omgekeerd is het van belang dat overheden gebruik kunnen blijven maken ICT diensten van organisaties die alleen via IPv6 bereikbaar zijn.
- De beheerslasten nemen af door vereenvoudigd management van IP adressen.
- Het verbeteren van de interoperabiliteit: er is geen NAT meer nodig. Toegang tot de basisregistraties (GBA, etc) wordt bijvoorbeeld makkelijker gemaakt binnen de overheid, omdat de NAT problematiek verdwijnt en via vereenvoudigde firewall-regels de toegang geregeld kan worden.
- IPv6 maakt expansie van internetworking mogelijk naar vele miljarden devices. Binnen IPv4 is dit niet mogelijk vanwege de te beperkte adresruimte.

5 Advies aan Forum en College

5.1 Samenvatting van de toetsingscriteria

Samengevat is het oordeel op de toetsingscriteria als volgt:

– *Openheid*

De standaard voldoet in voldoende mate aan de criteria van openheid. Men kan vrij over de standaard beschikken, er liggen geen Intellectual Property Rights (IPR) op de standaard en de IETF is een open organisatie die voor beheer en onderhoud van de standaarden zorgt.

– *Bruikbaarheid*

De standaard voldoet aan de criteria van bruikbaarheid. IPv6 is een volwassen standaard, waarmee voldoende praktijkervaring is opgedaan. Er is verder voldoende ondersteuning bij productleveranciers, terwijl het aanbod bij dienstenleveranciers beperkt is. De ondersteuning van IPv6 neemt in alle markten echter continue toe. Bij eindgebruikersorganisaties wordt IPv6 nog wel relatief weinig gebruikt.

– *Potentieel*

IPv6 zal bijdragen aan het verbeteren van de interoperabiliteit: er zijn nu interoperabiliteitsproblemen aan te wijzen tussen overheidspartijen onderling, die door inzet van IPv6 opgelost zouden kunnen worden. Er is geen impact op de leveranciers-onafhankelijkheid.

– *Impact*

De impact van IPv6 krijgt vooral gestalte bij de migratie van IPv4 naar IPv6. Daarbij is een structurele aanpak gewenst en moet IPv6 ingebed worden in de standaard processen van de organisatie. Er zal een situatie ontstaan waarin beide technologieën gebruikt worden, waarbij beheerslasten (onderhouden van twee technologieën) aanvankelijk toe zullen nemen. De expertgroep stelt vast dat het toepassen van IPv6 een belangrijk positief effect heeft op het realiseren van toegankelijkheid en bereikbaarheid van (overheids)diensten, waarmee continuïteit van de bedrijfsvoering ook voor de toekomst wordt gewaarborgd.

5.2 Advies

De expertgroep adviseert het college om IPv6 zonder voorwaarden op te nemen op de lijst met open standaarden voor "pas toe of leg uit", met het in hoofdstuk 2 vastgestelde toepassings- en werkingsgebied. Bij het advies voor opname van IPv6 wordt aangetekend dat IPv4 de nu gangbare versie van de standaard is. Omwille van interoperabiliteit is het in alle gevallen raadzaam om voorlopig naast IPv6 ook IPv4 te (blijven) ondersteunen ("dual stack").

De expertgroep is op basis van de geïdentificeerde risico's echter van mening dat opname van IPv6 op de lijst met open standaarden weliswaar noodzakelijk, maar op zichzelf onvoldoende is om adoptie en ingebruikname van IPv6 te realiseren. Het "pas toe of leg uit" principe ziet namelijk alleen toe op aanschaf en niet op het daadwerkelijke gebruik van IPv6 in ICT systemen. Opname op de lijst creëert dus een zekere urgentie, maar naar de mening van de expertgroep zijn vervolgacties nodig om deze urgentie te vertalen naar (meer) activiteit bij de organisaties op wie deze lijst van toepassing is, om daadwerkelijk gebruik van IPv6 te stimuleren en de risico's die daarbij optreden te ondervangen.

Voor een effectieve uitrol van IPv6 binnen de overheid adviseert de expertgroep het Forum daarom aanvullend om:

- De sense of urgency voor de uitrol van IPv6 te communiceren. Bijvoorbeeld door het gebruik van IPv6 actief te promoten binnen de overheid als een voorwaarde voor interoperabiliteit.
- De noodzaak voor actieve ondersteuning van overheidsorganisaties onder de aandacht te brengen. Daarbij moet duidelijk zijn dat kennis over IPv6 en de impact hiervan op systeem- en netwerkbeheer van groot belang is. Verder is ondersteuning van inkoop bij de overheid mogelijk gewenst. Richtlijnen voor gebruik, een kennishandreiking of een support centrum zijn oplossingen die invulling kunnen geven aan kennisoverdracht richting organisatieonderdelen die zich met inkoop- en beheerstaken bezig houden.
- Onder de aandacht te brengen dat IPv6 een integraal onderdeel moet zijn van de netwerkinfrastructuur binnen de overheid. In best practices moet worden gewezen op het belang van het configureren en in gereedheid brengen van IPv6 bij vervanging/uitbreiding van systemen. Dit zorgt voor een beheersbaar migratiepad naar IPv6.
- Ervaringen bij implementatietrajecten te laten delen. Het delen van ervaringen tussen overheidsorganisaties onderling kan acceptatie en adoptie bespoedigen en veelvoorkomende en vaak generieke problematiek bij implementatie van IPv6 bespreekbaar en/of inzichtelijk maken voor alle betrokken partijen.
- Een organisatie aanwijzen om bovengenoemde activiteiten te coördineren en mogelijk in onder te brengen. Een nog op te bouwen expertisecentrum of de Nederlandse IPv6 Task Force kunnen deze rol op zich nemen.

6 Referenties

- [1] Internet Protocol, Version 6 (IPv6) Specification,
<http://tools.ietf.org/rfc/rfc2460.txt>
- [2] *Actieplan Nederland Open in Verbinding*, 's-Gravenhage:
Ministerie van Economische Zaken, 2007.
- [3] P.H. Minneché and L. Korsten, *Open Standaarden*,
Het proces om te komen tot een lijst met open standaarden,
Verdonck, Klooster & Associates B.V., 2008.
- [4] "IPv6 Monitoring in Nederland: De Nulmeting", juni 2010,
<http://www.rijksoverheid.nl/bestanden/documenten-en-publicaties/rapporten/2010/07/26/ipv6-monitoring-in-nederland-de-nulmeting/ipv6monitoring-ez-wp1-v2-whitepapaer-final.pdf>