**Forum Standaardisatie**

Wilhelmina v Pruisenweg 104
2595 AN Den Haag
Postbus 84011
2508 AA Den Haag
www.forumstandaardisatie.nl

# notitie

## COLLEGE STANDAARDISATIE CS08-11-02A

| | | | |
|---|---|---|---|
| **Agendapunt:** | 02 Lijst open standaarden | | |
| **Betreft:** | Advies over opname van combinatie IPv6 en IPv4 op lijst met open standaarden voor 'pas toe of leg uit' | | |
| **Aan:** | College Standaardisatie | | |
| **Van:** | Forum Standaardisatie | | |
| **Datum:** | 29 oktober 2010 | **Versie** | 1.0 |
| **Bijlagen:** | | | |

**Waarom is een keuze belangrijk?**
De standaard Internet Protocol versie 6 (IPv6) bepaalt dat ieder ICT-systeem binnen een netwerk een uniek nummer (IP-adres) heeft. IPv6 biedt ondersteuning voor veel meer adressen dan de tegenwoordig gangbare voorganger IPv4. Op dit moment is het restant aan IPv4-adressen zeer beperkt. Daardoor kan de interoperabiliteit tussen systemen op relatief korte termijn (ong. 2 jaar) niet meer gegarandeerd worden. Delen van het internet (in zowel binnen- als buitenland) zullen door het tekort namelijk "IPv6-only" worden. De desbetreffende systemen zijn alleen bereikbaar via IPv6 en kunnen niet communiceren met systemen die alleen IPv4 gebruiken. Dit zal ook de (semi-)publieke sector raken. Het is daarom cruciaal dat de (semi-) publieke sector tijdig investeert in IPv6.

**Kunt u met een gerust hart "ja"zeggen?**
Het voorliggende advies is het resultaat van een uitgebreid expertonderzoek, een publieke consultatie en bespreking in het Forum Standaardisatie. IPv6 is niet backwards compatible met IPv4. Beide standaarden kunnen, zullen en moeten naar de mening van de expertgroep de komende periode (10 tot 20 jaar) naast elkaar, binnen hetzelfde netwerk gebruikt worden. Hoewel de expertgroep heeft onderkend dat IPv6 naast IPv4 ingezet moet worden, heeft de expertgroep strikt genomen alleen geadviseerd over de opname van IPv6. Het advies van het Forum is om de combinatie van beide versies op te nemen op de "pas toe of leg uit"-lijst. Daardoor wordt bestaande interoperabiliteit op basis van IPv4 niet in gevaar gebracht. Tegelijkertijd opent het de deur naar de aanvullende interoperabiliteitsmogelijkheden van IPv6.

**Zijn er risico's verbonden aan de keuze?**
Ingebruikname van IPv6 heef een aanzienlijke impact op de infrastructuur. Er zal een situatie ontstaan waarin zowel IPv4 als IPv6 naast elkaar gebruikt worden, waarbij beheerslasten (onderhouden van twee technologieën) aanvankelijk toe zullen nemen en beheerstaken complexer zullen worden. Verder onderkent de expertgroep een aantal mogelijke risico's met betrekking tot beveiliging van netwerken en privacy van IPv6-gebruikers. Voor deze risico's bestaan echter effectieve maatregelen. Voor goede toepassing van IPv6 is het cruciaal dat expertise en ervaring opgedaan en gedeeld worden.

**Doel**



Het College Standaardisatie wordt gevraagd in te stemmen met:

1. de opname van de combinatie van IPv6 en IPv4 op de lijst met open standaarden voor 'pas toe of leg uit'.;
2. het volgende functioneel toepassingsgebied: "Communicatie op netwerkniveau over organisatiegrenzen heen tussen organisaties, individuele eindgebruikers, apparaten, diensten en sensoren";
3. het volgende organisatorisch werkingsgebied: "Overheden en instellingen uit de (semi-) publieke sector";
4. het oproepen van het Ministerie van Economische Zaken om een kenniscentrum op te richten dat zorgt voor het communiceren van de "sense of urgency", het delen van expertise en ervaringen, en het gericht doorverwijzen voor actieve ondersteuning.
5. het oproepen van Ministerie van Binnenlandse Zaken en Koninkrijksrelaties om er voor te zorgen dat de standaarden worden opgenomen in de interne netwerk- en systeeminfrastructuur van de overheid en in voorzieningen van de e-Overheid.

**Toelichting**

*Ad. 1 Opname op de "pas toe of leg uit"-lijst*
Internet Protocol versie 6 (IPv6) maakt communicatie van data tussen ICT-systemen binnen een netwerk, zoals internet, mogelijk. De standaard IPv6 kan daarbij worden beschouwd als een verzamelnaam voor een aantal samenhangende standaarden, die zijn vastgelegd in zogenaamde RFC's[1]. De IPv6 standaard wordt beheerd en onderhouden door de Internet Engineering Task Force (IETF), een non-profit organisatie die Internetstandaarden ontwikkelt. De huidige (kern)specificatie is gepubliceerd in 1998.

Toevoeging van IPv6 in combinatie met IPv4 aan de lijst met open standaarden voor 'pas toe of leg uit' betekent dat van alle (semi-) publieke organisaties wordt verwacht dat zij voor deze standaard een 'pas-toe-of-leg uit' beleid gaan hanteren. Dat betekent dat nieuw aan te schaffen apparatuur met beide standaarden overweg moet kunnen. "Dual stack", dat staat beschreven in RFC4213, is in de praktijk het meest voor de hand liggende mechanisme om beide versies te ondersteunen.

IPv6 is nu (evenals IPv4) opgenomen op de lijst met gangbare open standaarden. Beide standaarden zullen van deze lijst worden verwijderd.

Door een expertgroep is IPv6 beoordeeld op de criteria: openheid, potentieel, bruikbaarheid en impact. Over alle vier de criteria is positief geadviseerd. Tijdens de publieke consultatieronde zijn achttien reacties op het expertadvies ontvangen, waarvan elf reacties een inhoudelijke terugkoppeling gaven op het rapport. De meest belangrijke reactiepunten komen terug onder "Schets van de expertgroep en de consultatie". De inhoudelijke reacties zijn met name aanvullend van aard en zijn verwerkt in dit Forum-advies. Geen van de reacties heeft aanleiding gegeven tot het herzien van het expertadvies.

Om interoperabiliteit te waarborgen kunnen, zullen en moeten beide standaarden (IPv4 en IPv6) naar de mening van de expertgroep de komende periode naast elkaar, binnen hetzelfde netwerk gebruikt worden. Om die reden worden beide als combinatie opgenomen op de lijst met open standaarden voor "pas toe of leg uit".

[1] *Request for Comments, het standaard publicatieformaat voor de Internet Standaarden van de IETF.*

*Ad. 2 en 3 Functioneel toepassingsgebied en organisatorisch werkingsgebied*
Het functioneel toepassingsgebied is door de expertgroep gedefinieerd als: "communicatie op netwerkniveau over organisatiegrenzen heen tussen organisaties, individuele eindgebruikers, apparaten, diensten en sensoren".

Hierbij dient expliciet te worden opgemerkt, dat het toepassingsgebied van IPv6 het werkzame koppelvlak tussen organisaties is, d.w.z. dat IPv6 als standaard ingezet moet worden óver organisatiegrenzen heen, in de communicatie aan de buitenkant.

Het organisatorisch werkingsgebied is als volgt gedefinieerd: "Overheden en instellingen uit de (semi-) publieke sector", zoals vastgelegd in het actieplan "Nederland Open in Verbinding".

*Ad. 4 en 5 Aanvullende acties ter bevordering adoptie*
De expertgroep is van mening dat opname van IPv6 op de lijst met open standaarden weliswaar noodzakelijk is, maar op zichzelf onvoldoende is om adoptie en ingebruikname van IPv6 daadwerkelijk te realiseren. Voor een effectieve uitrol van IPv6 binnen de overheid adviseert de expertgroep het Forum daarom aanvullend om een aantal acties te ondernemen en bijhorende actiehouders te benoemen. Onderstaande aanbevolen acties zijn een verdere uitwerking van de aanbevelingen die zijn benoemd in het expertadvies.

- *Communiceer "sense of urgency"*
  Communiceer de "sense of urgency" voor de uitrol van IPv6, bijvoorbeeld door het gebruik van IPv6 actief te promoten binnen de overheid als een voorwaarde voor interoperabiliteit. Maak tegelijkertijd ook de risico's en concrete gevolgen van niet-tijdelijke migratie en uitrol duidelijk. De huidige communicatieactiviteiten zijn beperkt qua omvang en versnipperd over meerdere organisaties als de IPv6 Task Force en Govcert. Het Ministerie van EZ kan er als opdrachtgever van de Task Force en Govcert op aansturen, dat communicatie toeneemt en meer gericht wordt op het creëren van de "sense of urgency".

- *Deel expertise en ervaringen*
  Het delen van ervaringen tussen overheidsorganisaties onderling en met het bedrijfsleven kan de adoptie bespoedigen en veelvoorkomende, vaak generieke problematiek bij implementatie van IPv6 inzichtelijk maken voor alle betrokken partijen. De huidige IPv6 Task Force is op dit moment al een organisatie om ervaringen uit te wisselen, met name tussen partijen uit het bedrijfsleven. De actieve betrokkenheid van overheidsorganisaties is beperkt. Het Ministerie van EZ kan als opdrachtgever van de huidige IPv6 Task Force de betrokkenheid van andere overheidsorganisaties stimuleren.

- *Organiseer actieve ondersteuning*
  Overheidsorganisaties hebben niet alle kennis over IPv6 in huis. De IPv6 Task Force kan als startpunt of loket fungeren voor het bieden van ondersteuning, maar verzorgt daarbij zelf niet de ondersteuning. Er zijn partijen in de markt die zich richten op het geven van opleidingen en trainingen over IPv6. Het zevende kader project 6DEPLOY is daarnaast een project van de EU, dat toegang geeft tot een database met organisaties die trainingen verzorgen.

- *Opname in de interne netwerk- en systeeminfrastructuur*
  Zorg ervoor dat IPv6 een integraal onderdeel is van de netwerk- en systeeminfrastructuur binnen de (semi-)publieke sector (denk o.a. aan:

Diginetwerk, SUWInet, Gemnet). Vanuit ICCIO kan men erop aansturen dat de uitrol van IPv6 wordt ingebed in de standaardprocessen van de Rijksoverheid. KING en BZK kunnen een arrangement opstellen over inbedding op gemeentelijk niveau. Het Ministerie van BZK kan er als opdrachtgever van aanbestedingen van SBO-ICM voor zorgen, dat IPv6 in de ICT-raamovereenkomsten (o.a. EASI en de nieuwe hosting-mantel) wordt opgenomen.

- *Opname in voorzieningen e-Overheid*
  Het Ministerie van BZK heeft als beleidsopdrachtgever van Logius een taak om ervoor te zorgen dat voorzieningen van de e-Overheid (Digipoort, DigiD, etc.) daadwerkelijk IPv6 ondersteunen.

**Welk probleem wordt daarmee opgelost?**
IPv6 lost het probleem van het voorziene tekort aan internetadressen op. In de huidige situatie worden overheidsdiensten overwegend ontsloten door middel van het gebruik van IPv4. Op dit moment is het restant aan IPv4 adressen echter zo beperkt, dat interoperabiliteit tussen systemen op relatief korte termijn (ong. 2 jaar) in grote delen van de wereld niet meer gegarandeerd kan worden. Delen van het internet (in zowel binnenland als buitenland) zullen door het tekort alleen via IPv6 te bereiken zijn. Als overheidsorganisaties alleen IPv4 blijven gebruiken zullen diensten van de overheid niet meer voor deze IPv6-only partijen bereikbaar zijn en is communicatie van de overheidsorganisaties met deze IPv6-only organisaties niet meer mogelijk.

De expertgroep constateert daarbij dat de standaard met name een bijdrage levert aan het vergroten van interoperabiliteit met overheidsorganisaties en geen additionele bijdrage levert aan leveranciersonafhankelijkheid.

**Waar gaat het inhoudelijk over?**
Internet Protocol versie 6 (IPv6) voorziet met name in een adresseringsmechanisme dat noodzakelijk is om de data tussen ICT-systemen te kunnen uitwisselen. De standaard IPv6 kan daarbij worden beschouwd als een verzamelnaam voor een aantal samenhangende standaarden, die zijn vastgelegd in zogenaamde RFC's[2].

De kern van de IPv6 standaard is daarbij gespecificeerd in RFC 2460. De in het expertadvies behandelde verzameling van RFC's specificeert verder op hoofdlijnen (1) welke RFC's altijd geïmplementeerd moeten worden om de kernfunctionaliteit van IPv6 te realiseren, (2) de eisen die gesteld worden aan IPv6 nodes en (3) mechanismen voor de transitie van IPv4 naar IPv6 en mechanismen om co-existentie en compatibiliteit met IPv4 te bewerkstelligen. IPv6 is ontwikkeld als de natuurlijke opvolger van het huidige Internet Protocol IPv4 en biedt als belangrijkste voordeel een (veel) grotere adresruimte. Aangezien de standaard IPv6 ook een volledige herziening van het Internet Protocol betreft, is parallel ook gewerkt aan eenvoudiger beheer en betere ondersteuning van beveiliging. Communicatie tussen alle denkbare 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.

**Zijn er alternatieven voor de voorgestelde keuze?**
De expertgroep stelt vast, dat IPv4 binnen het gekozen toepassingsgebied 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

[2] *Idem*

van IPv4 en zal op termijn uitgroeien tot de de-facto standaard voor end-to-end communicatie op basis van het Internet Protocol.

**Schets van de expertgroep en de consultatie**
De leden van de expertgroep waren afkomstig van belanghebbende organisaties uit zowel de private als publieke sector, waaronder het Ministerie van BZK, Logius en de Belastingdienst, de Rabobank, TNO, KPN, XS4ALL, Stratix, Surfnet, Randstad, onderzoeks- en ontwikkelingsgroep NLnet Labs, netwerkarchitectenbedrijf NiVo, GNKS Consult en de voorziening tot samenwerking Politie Nederland (vtsPN). In haar bijeenkomst op 22 juli heeft de expertgroep IPv6 getoetst aan de criteria voor opname op de lijst, en is tot de conclusie gekomen dat opname wenselijk is. Na opstelling van het rapport heeft een openbare consultatie plaatsgevonden. Tijdens de publieke consultatieronde zijn achttien reacties ontvangen, waarvan elf een inhoudelijke terugkoppeling gaven op het expertadvies.

*Overzicht meest belangrijke opmerkingen consultatie*

- Impact op bedrijfsvoering: een van de criteria is de impact die de standaard heeft op de bedrijfsvoering. In twee reacties wordt aangegeven dat er vraagtekens kunnen worden gezet bij de toegankelijkheid van overheidssites en -diensten wanneer de IPv4-adressen opraken. Hierbij wordt benadrukt dat systemen die alleen van een IPv6-adres worden voorzien, niet uitgesloten zouden mogen worden van communicatie met de overheid. In het expertadvies wordt eveneens gesteld dat het toepassen van IPv6 een belangrijk en positief effect heeft op ondermeer de toegankelijkheid en bereikbaarheid van overheidsdiensten. Meer expliciet kan ook worden gesteld, dat IPv6 zelfs een noodzakelijke voorwaarde is om ook in de toekomst de continuïteit van de overheidsbedrijfsvoering richting alle burgers en bedrijven te blijven waarborgen en daarbij geen burgers en bedrijven uit te sluiten.
- Impact op privacy en veiligheid: een van de criteria is de impact die de standaard heeft op de privacy en veiligheid. In twee reacties wordt benadrukt dat de introductie van IPv6 aanvullende risico's op het gebied van privacy met zich mee kan brengen, door de zichtbaarheid van de individuele endpoints en de mogelijkheid om een koppeling te leggen tussen een IPv6-adres en het bijbehorende fysieke object. In het expertadvies worden deze risico's ook onderkend. Daarbij wordt in het advies aangegeven, dat IPv6 oplossingen voor dit probleem biedt, maar dat deze oplossingen altijd geactiveerd en ingesteld moeten worden. In implementatietrajecten moet volgens de expertgroep voor de hiergenoemde risico's en de bijbehorende oplossingen ruime aandacht zijn.
- Impact en migratie: een van de criteria voor impact is het gemak waarmee naar de standaard kan worden gemigreerd. In twee reacties wordt aangegeven dat migratie alleen kan plaats vinden als er een "dual-stack" situatie wordt gecreëerd, waarbij IPv6 de komende jaren gebruikt wordt náást IPv4. Het expertadvies stelt eveneens vast, dat er maar één waarschijnlijk migratiescenario mogelijk is; de migratie van IPv4-only naar co-existentie van IPv6 en IPv4 in een "dual-stack" situatie. De expertgroep verwacht daarbij, dat de komende 10-20 jaar IPv4 en IPv6 gelijktijdig gebruikt zullen gaan worden.
- Impact en migratie (2) : In drie reacties wordt aangegeven dat een migratie naar IPv6 baat heeft bij een geleidelijke invoering waarbij het noodzakelijk is om de netwerkinfrastructuur op natuurlijke vervangingsmomenten gereed te maken. Het expertadvies ondersteunt deze reacties, door eveneens te stellen dat een eventuele invoering gefaseerd moet worden uitgevoerd. De expertgroep heeft daarbij aangegeven, dat invoering van IPv6 van meet af aan moet worden meegenomen in de reguliere activiteiten van de lijnorganisatie. In

overeenstemming met de reacties is de expertgroep van mening, dat hiermee een kostenefficiënte migratie kan worden uitgevoerd: een onevenredig dure inhaalslag later kan worden voorkomen en de meerkosten kunnen over de tijd worden verdeeld.

- Bruikbaarheid : een van de criteria voor bruikbaarheid is de praktijkervaring met het gebruik van de standaard. In een reactie wordt gewezen op het feit dat gebruik van IPv6 binnen de Nederlandse (semi-)publieke sector zo goed als afwezig is. Dit is een zinvolle aanvulling op het expertadvies, waarin met name gewezen wordt op de ervaring van instellingen en organisaties buiten de Nederlandse (semi-)publieke sector. Binnen de (semi-)publieke sector heeft met name SURFnet ervaring opgedaan. Een ander criterium voor bruikbaarheid is de mate van ondersteuning door marktpartijen. In een reactie wordt gesteld dat de problemen bij productondersteuning zich met name op het niveau van de applicaties zullen voordoen. Dit is een zinvolle verduidelijking van het expertadvies, waar alleen in de business case wordt aangegeven dat het testen van applicaties op geschiktheid voor IPv6 als potentieel tweede kostenpost wordt gezien bij een migratie naar IPv6.
- Advies ten aanzien van expertisecentrum : In twee reacties worden suggesties gedaan ten aanzien van het aanvullend advies van de expertgroep. Hierbij wordt gewezen op de noodzaak om ook de concrete gevolgen van een niet-tijdige uitrol te communiceren. Dit is een zinvolle aanvulling op het expertadvies, waarin alleen het uitdragen van de urgentie van een tijdelijke uitrol wordt geadviseerd. Daarnaast wordt in een reactie gewezen op het nut van een expertisecentrum dat zowel overheid als bedrijfsleven van dienst is. In aanvulling op de aanbeveling om een expertisecentrum in te richten, kan worden gesteld dat in een dergelijk expertisecentrum zowel overheidspartijen als bedrijven deel moeten nemen om ervaringen niet alleen tussen overheden onderling, maar ook tussen overheden en bedrijfsleven uit te kunnen wisselen.
- Advies ten aanzien van ondersteuning : In twee reacties wordt het belang van bijscholing en het aanreiken van aanvullende kennis voor o.m. systeem- en netwerkbeheerders benadrukt. In het expertadvies wordt eveneens aangegeven dat een kennishandreiking een onderdeel zou moeten zijn van een actieve ondersteuning van overheidsorganisaties. Verder wordt het belang van opleiding van IT-medewerkers en -staf benadrukt in de business case van het expertadvies, waar deze activiteit als potentieel grootste kostenpost wordt gezien bij migratie naar IPv6.

**Mogelijke consequenties van opname op de lijst met standaarden**
Consequentie van opname van IPv6 op de lijst met open standaarden voor "pas toe of leg uit", is een verplichting om IPv6 toe te passen op het werkzame koppelvlak tussen organisaties, d.w.z. dat IPv6 als standaard ingezet moet worden over organisatiegrenzen heen, in de communicatie met de buitenwereld. IPv6 vindt zijn toepassing daarbij náást IPv4 en niet als vervanging van IPv4, omdat co-existentie in "dual-stack" naar de mening van de expertgroep het enige zinnige migratiescenario is. In een "dual-stack situatie" zullen gedurende een lange periode (10-20 jaar) IPv4 en IPv6 naast elkaar gebruikt gaan worden op de koppelvlakken van de organisaties. Overheidsdiensten zullen dan dus zowel via IPv4 als IPv6 te benaderen en bereiken zijn. Bij deze migratie is wel expliciet aandacht vereist voor een gestructureerde en gefaseerde aanpak.

**Communicatie**
Zowel het Forum Standaardisatie als het Programmabureau Nederland Open in Verbinding zal aandacht besteden aan de opname van IPv6 op de lijst met open standaarden voor "pas toe of leg uit".