

VERDUIDELIJKING FUNCTIONEEL TOEPASSINGSGEBIEDEN

Eindrapport

VERDUIDELIJKING FUNCTIONEEL TOEPASSINGSGEBIEDEN

Eindrapport

Rick van Rooijen

DATUM	7 april 2017
STATUS	Definitief
VERSIE	1.0
PROJECTNUMMER	20163239OUFTVS
INTERNE TOETS	Jasmijn Wijn

INHOUDSOPGAVE

Inhoudsopgave	3
1 Inleiding	5
1.1 Achtergrond en aanleiding	5
1.2 Doel en scope van dit document	9
1.3 Doelgroep	10
1.4 Doorlopen proces	10
1.5 Leeswijzer	10
2 Huidige omschrijvingen	12
2.1 Inleiding	12
2.2 Kenmerkende elementen	12
2.3 Verplichten, toestaan of niet toestaan	14
2.4 Ideaaltypische syntactische structuur	15
2.5 Conclusies en aanbevelingen	17
3 Nieuwe omschrijvingen	19
3.1 Inleiding	19
3.2 Geselecteerde standaarden	19
3.3 Specifieke verplichtingen	20
3.4 Nieuwe omschrijvingen	25
3.5 Conclusies en aanbevelingen	30
4 Vervolgaanpak	32
4.1 Inleiding	32
4.2 Scenario's	32
4.3 Resterende standaarden	33
4.4 Aanpak	35
4.5 Planning	35
4.6 Conclusies en aanbevelingen	36
BIJLAGEN	38
A Voorbeelden van kenmerkende elementen	39
A1. Functionaliteit ICT-dienst of -product	39
A2. Soort ICT-dienst of -product	39
A3. Gebruiksdoel ICT-dienst of -product	40

A4.	Gebruikskader ICT-dienst of -product	40
A5.	Gebruikers ICT-dienst of -product	41
A6.	Werking standaard	41
A7.	Naam standaard	42
A8.	Nut standaard	42
A9.	Uitzondering/uitsluiting	43
B	Scores voor duidelijkheid	44
C	Toets ideaaltypische syntactische structuur	47
C1.	BWB	47
C2.	Digikoppeling 2.0	48
C3.	DigiToegankelijk (EN 301 549 met WCAG 2.0)	49
C4.	DNSSEC	50
C5.	HTTPS en HSTS	50
C6.	SETU	51
C7.	StUF	52
C8.	TLS	52

1 INLEIDING

In opdracht van het Forum Standaardisatie heeft Verdonck, Klooster & Associates (VKA) de omschrijvingen van de functioneel toepassingsgebieden van de verplichte standaarden op de lijst met open standaarden onderzocht en voorstellen gedaan hoe deze te verduidelijken en meer richting te geven in de discussie over het functioneel toepassingsgebied. De uitkomsten van dit onderzoek zijn samengevoegd in dit eindrapport. In dit inleidende hoofdstuk wordt allereerst uitgebreid ingegaan op de achtergrond en aanleiding van het onderzoek. Vervolgens komen doel, scope en doelgroep van dit document aan bod en wordt beschreven op welke wijze het onderzoek is uitgevoerd. Het hoofdstuk wordt afgesloten met een leeswijzer.

1.1 Achtergrond en aanleiding

1.1.1 De toepassings- en werkingsgebieden van standaarden

De lijst met open standaarden bevat twee typen standaarden, namelijk standaarden die verplicht zijn krachtens het 'pas toe of leg uit' beleid en standaarden die zijn aanbevolen, omdat ze gangbaar zijn of in opkomst en veelbelovend. In dit onderzoek richten we ons op de verplichte ('pas toe of leg uit') standaarden.

Het 'pas toe of leg uit' beleid¹ verplicht (overheids)organisaties ertoe om bij de aankoop, inhuur en ontwikkeling van ICT-producten en -diensten in beginsel de van toepassing zijnde open standaarden te gebruiken. Dit wordt nader uitgewerkt in paragraaf 1.1.3 over de Instructie rijksdienst bij aanschaf ICT-diensten of ICT-producten.

Om te kunnen beoordelen welke open standaarden van toepassing zijn, en dus moeten worden uitgevraagd bij een aanbesteding, zijn voor iedere standaard die verplicht is, een 'functioneel toepassingsgebied' en een bijbehorend 'organisatorisch werkingsgebied' bepaald. Wat met deze begrippen wordt bedoeld wordt hieronder uiteengezet.

Over de omschrijvingen van het functioneel toepassingsgebied en het organisatorisch werkingsgebied is altijd de nodige discussie, omdat deze omschrijvingen bepalend zijn voor de vraag of een (overheids)organisatie een standaard wel of niet moet hanteren. Onduidelijkheid hierover kan dan ook de adoptie van een standaard in de weg staan.

OVER HET TOEPASSINGSGEBIED

Het functioneel toepassingsgebied van een standaard bepaalt voor welke ICT-producten en -diensten de standaard relevant is en wanneer deze dus moet worden toegepast. Dit kunnen zeer uiteenlopende ICT-producten en -diensten zijn. Wat de ICT-producten en -diensten gemeen

¹ <http://wetten.overheid.nl/jci1.3:c:BWBR0024717&z=2008-11-23&g=2008-11-23>

hebben, is dat zij kunnen worden gebruikt om digitale gegevens uit te wisselen tussen overheden onderling of tussen overheden en burgers of bedrijven. Het 'pas toe of leg uit' beleid geldt immers alleen voor de uitwisseling van digitale gegevens door overheden met burgers, bedrijven en andere overheden. De verplichting geldt niet voor gegevensuitwisseling binnen één en dezelfde organisatie.

Het functioneel toepassingsgebied van een standaard zou iets moeten zeggen over de ICT-producten en -diensten waarvoor de standaard relevant is. Dit is niet altijd het geval. Zo wordt bij sommige standaarden op de lijst de werking of het nut van de standaard beschreven. Dit zorgt voor onduidelijkheid, wat adoptie van standaarden kan belemmeren.

Voorbeeld: huidige omschrijvingen die duidelijker kunnen

- ✗ Digikoppeling 2.0: 'Geautomatiseerde gegevensuitwisseling tussen informatiesystemen voor sectoroverstijgend berichtenverkeer, op basis van drie koppelvlakstandaarden:
 - DK ebMS standaard voor meldingen tussen informatiesystemen
 - DK WUS standaard voor de bevraging van informatiesystemen
 - DK GB standaard voor de uitwisseling van grote berichten'
- ✗ TLS: 'Het met behulp van certificaten beveiligen van de verbinding (op de transportlaag) tussen client- en serversystemen of tussen serversystemen onderling, voor zover deze gerealiseerd wordt met internettechnologie.'

Voorbeeld: nieuwe omschrijvingen die duidelijker zijn

- ✓ Digikoppeling 2.0: 'Digikoppeling moet worden toegepast op alle digitale gegevensuitwisseling met behulp van gestructureerde berichten die plaatsvindt met voorzieningen die onderdeel zijn van de GDI, waaronder de basisregistraties, of die sectoroverstijgend is.'
- ✓ TLS: 'TLS moet worden toegepast op de uitwisseling van gegevens tussen clients en servers en tussen servers onderling voor zover deze uitwisseling over internet plaatsvindt.'

Voorbeeld: huidige omschrijvingen die al duidelijk zijn

- ✓ SETU: 'De elektronische berichtenuitwisseling rondom de bemiddeling/inhuur van flexibele arbeidskrachten.'
- ✓ SMeF 2.0: 'De verzending van elektronische facturen door organisaties die deelnemen aan het economisch verkeer in Nederland (waaronder overheden) en de ontvangst hiervan door overheden.'

Duidelijkheid over wat wel en wat niet onder functioneel toepassingsgebied wordt verstaan is tot dusver niet expliciet gegeven. Vandaar dat hier nu onderzoek naar is gedaan.

OVER HET WERKINGSGBIED

Het organisatorisch werkingsgebied bepaalt voor welke organisaties de verplichting geldt. Dit werkingsgebied is over het algemeen breed geformuleerd: 'Overheden (Rijk, provincies, gemeenten en waterschappen) en instellingen uit de (semi-)publieke sector'.

Met Rijk wordt bedoeld de ministeries, de uitvoerende diensten die onder deze ministeries vallen (denk aan de Belastingdienst), de inspecties (zoals de Onderwijsinspectie) en de Hoge Colleges van Staat. Voorbeelden van de Hoge Colleges van Staat zijn de Eerste en Tweede Kamer der Staten Generaal, de Algemene Rekenkamer en de Nationale ombudsman².

Bij instellingen uit de (semi-)publieke sector gaat het onder meer om zelfstandige bestuursorganen, zoals de Kamers van Koophandel, de Sociale Verzekeringsbank (SVB) en het Centraal Bureau Rijvaardigheidsbewijzen (CBR)³.

Ook private instellingen kunnen belast zijn met een publieke taak. Denk bijvoorbeeld aan zorginstellingen, zoals ziekenhuizen, en aan scholen en universiteiten. Ook voor deze organisaties kan de verplichting gelden⁴.

Het functioneel toepassingsgebied en het bijbehorende organisatorisch werkingsgebied bepalen samen of een (overheids)organisatie een open standaard moet gebruiken of niet. Over het functioneel toepassingsgebied is regelmatig discussie, meer dan over het organisatorisch werkingsgebied. In dit onderzoek richten we ons daarom op de functioneel toepassingsgebieden van de standaarden.

² <https://www.werkenvoornederland.nl/over-de-rijksoverheid/wat-is-de-rijksoverheid>

³ <https://www.rijksoverheid.nl/onderwerpen/rijksoverheid/inhoud/zelfstandige-bestuursorganen>

⁴ <https://www.forumstandaardisatie.nl/thema/open-standaarden>

1.1.2 Behoefte aan meer duidelijkheid, uniformiteit en consistentie

Over de functioneel toepassingsgebieden van de standaarden op de lijst met open standaarden is regelmatig discussie. Niet alleen tijdens de toetsingsprocedure, wanneer de omschrijving van het functioneel toepassingsgebied wordt bepaald. Ook na de opname van een standaard op de lijst ontvangt het Bureau Forum Standaardisatie regelmatig vragen over het functioneel toepassingsgebied dat hierbij wordt vermeld. Onduidelijke of vage beschrijvingen moeten daarom vermeden worden.

Gebruikers van de lijst, zoals bestuurders, architecten en inkopers van ICT, hebben aangegeven behoefte te hebben aan omschrijvingen van functioneel toepassingsgebieden die:

- duidelijk maken wanneer een standaard moet worden toegepast;
- uniform zijn aan de omschrijving van andere functioneel toepassingsgebieden;
- consistent zijn met andere afspraken.

Opgemerkt zij dat de behoefte aan meer uniformiteit van belang is, maar onderschikt aan de behoefte aan meer duidelijkheid en consistentie.

1.1.3 Rijksinstructie

De behoefte aan omschrijvingen die duidelijk maken wanneer open standaarden moeten worden toegepast, moet worden gezien in het licht van de Instructie rijksdienst bij aanschaf ICT-diensten of ICT-producten (kortweg Rijksinstructie)⁵. Deze instructie schrijft voor dat bij de aanschaf van een ICT-dienst of ICT-product voor een toepassingsgebied dat voorkomt op de lijst met verplichte standaarden van het Forum Standaardisatie, wordt gekozen voor een ICT-dienst of ICT-product dat gebruik maakt van een bij het desbetreffende toepassingsgebied vermelde open standaard.

Doordat de Rijksinstructie verwijst naar de toepassingsgebieden op de lijst met open standaarden, wordt de inhoud van de verplichting die van de Rijksinstructie uitgaat mede bepaald door de omschrijvingen van de functioneel toepassingsgebieden. Het is dan ook belangrijk dat functioneel toepassingsgebieden zo worden omschreven dat duidelijk is wanneer hiervoor ICT-diensten of ICT-producten worden aangeschaft.

Wanneer een standaard moet worden toegepast, kan alleen duidelijk worden gemaakt door het functioneel toepassingsgebied van de standaard te omschrijven aan de hand van de functionaliteit of de functionaliteiten van de ICT-dienst of het ICT-product dat de betreffende standaard dient te gebruiken. Dit is momenteel niet altijd het geval. Zo wordt bij sommige standaarden op de lijst de werking (functionaliteit) of het nut van de standaard beschreven. Dit leidt tot onduidelijkheid, wat adoptie van standaarden kan belemmeren.

⁵ <http://wetten.overheid.nl/jci1.3:c:BWBR0024717&z=2008-11-23&g=2008-11-23>

1.1.4 Bestuurlijke afspraken Nationaal Beraad

Niet alleen de behoefte aan meer duidelijkheid is aanleiding om eens goed naar de omschrijvingen van de functioneel toepassingsgebieden te kijken. Ook externe ontwikkelingen geven hier reden toe. Eén van deze ontwikkelingen zijn de bestuurlijke afspraken die worden gemaakt in het Nationaal Beraad Digitale Overheid (kortweg Nationaal Beraad).

In het Nationaal Beraad kunnen bestuurlijke afspraken worden gemaakt over de standaarden op de lijst met open standaarden. In het Nationaal Beraad van 2 februari 2016 zijn bijvoorbeeld aanvullende resultaatafspraken gemaakt over de adoptie van de informatieveiligheidsstandaarden TLS, DNSSEC, DMARC, SPF en DKIM. Op deze resultaatafspraken wordt in hoofdstuk 3 van dit rapport nog nader ingegaan.

De bestuurlijke afspraken en functioneel toepassingsgebieden kunnen met elkaar samenhangen en zullen inhoudelijk elkaar op moeten worden afgestemd.

1.1.5 Wet GDI

Ten slotte is er de Wet generieke digitale infrastructuur (Wet GDI), die de regering in tranches tot stand brengt. De eerste tranche, die op het moment van schrijven ter consultatie voorligt⁶, regelt de toegang tot elektronische dienstverlening en standaarden voor elektronisch verkeer.

Artikel 2 lid 2 van het wetsvoorstel bepaalt dat bij algemene maatregel van bestuur (AMvB) open standaarden kunnen worden aangewezen, die overheden dienen te hanteren in het elektronisch verkeer met andere overheden, met burgers en met bedrijven. Bij de aanwijzing dient het functionele toepassingsbereik van de standaard te worden omschreven.

Volgens de memorie van toelichting bij de Wet GDI zal een bij AMvB verplichte standaard van de lijst met verplichte standaarden worden verwijderd. Er kunnen echter redenen zijn om dit niet te doen, bijvoorbeeld omdat het toepassingsbereik van de algemene maatregel van bestuur kleiner is dan het functioneel toepassingsgebied of het organisatorisch werkingsgebied van de lijst met verplichte standaarden. Om inconsistenties en dubbel werk te voorkomen, dienen in zo'n geval de omschrijvingen op de lijst met verplichte standaarden en in de AMvB op elkaar te worden afgestemd.

1.2 Doel en scope van dit document

Dit document beschrijft de uitkomsten van het onderzoek dat VKA in opdracht van het Forum Standaardisatie heeft uitgevoerd naar de omschrijvingen van de functioneel toepassingsgebieden van de verplichte standaarden op de lijst met open standaarden. Het bevat zowel een analyse van de huidige omschrijvingen, als voorstellen voor nieuwe omschrijvingen en instrumenten om de

⁶ <https://www.internetconsultatie.nl/wetgdi>

omschrijvingen van functioneel toepassingsgebieden voor nu en in de toekomst te verduidelijken en te uniformeren.

1.3 Doelgroep

Dit document is geschreven voor het Forum Standaardisatie en de begeleiders van de procedure die standaarden doorlopen voordat deze op de lijst met open standaarden worden opgenomen.

Het Forum Standaardisatie wordt gevraagd om in te stemmen met de ideaaltypische syntactische structuur en de gevolgen hiervan voor gebruikers van de lijst (paragraaf 2.4) en met de vervolgaanpak (hoofdstuk 4). Vanwege haar rol in de toetsingsprocedure, wordt het Forum Standaardisatie aangeraden om ook kennis te nemen van de elementen waaruit de omschrijvingen kunnen zijn opgebouwd (paragraaf 2.2) en het advies om deze elementen al dan niet te gebruiken (paragraaf 2.3).

De procedurebegeleiders dienen kennis te nemen van de elementen waaruit de omschrijvingen kunnen zijn opgebouwd (paragraaf 2.2), het advies om deze elementen al dan niet te gebruiken (paragraaf 2.3) en de ideaaltypische syntactische structuur (paragraaf 2.4).

1.4 Doorlopen proces

De onderwerpen in dit document zijn eerst uitgewerkt in afzonderlijke notities. Deze en andere tussenresultaten zijn afgestemd met het Bureau Forum Standaardisatie en enkele externe adviseurs die bemoeienis hebben (of hebben gehad) met de standaarden waarvan het functioneel toepassingsgebied opnieuw is omschreven. Het Forum Standaardisatie is tussentijds geïnformeerd over de voortgang van het onderzoek tijdens de forumvergadering van 8 maart 2017. De onderzoeksresultaten zijn beschreven in dit eindrapport, dat aan het Forum Standaardisatie zal worden voorgelegd ter vaststelling.

1.5 Leeswijzer

Hoofdstuk 2 bevat een analyse van de omschrijvingen van de functioneel toepassingsgebieden van alle (in behandeling zijnde) standaarden. In dit hoofdstuk wordt ingegaan op de elementen waaruit de huidige omschrijvingen zijn opgebouwd. Vervolgens wordt aangegeven welke van deze elementen (kunnen) verduidelijken wanneer een standaard wel of niet moet worden toegepast. Op basis hiervan wordt per element geadviseerd om het gebruik hiervan verplicht te stellen, toe te staan of niet toe te staan. Ten slotte wordt een ideaaltypische syntactische structuur voorgesteld, die nu en in de toekomst kan helpen bij het vaststellen van toepassingsgebieden.

Hoofdstuk 3 bevat voor enkele geselecteerde standaarden een voorstel voor een nieuwe omschrijving. Hierbij is gebruik gemaakt van de ideaaltypische syntactische structuur en is rekening gehouden met verplichtingen die specifiek van toepassing zijn op de betreffende

standaarden. Alvorens over te gaan tot de nieuwe omschrijvingen, wordt ingegaan op de geselecteerde standaarden en de verplichtingen die specifiek voor deze standaarden gelden.

Hoofdstuk 4, ten slotte, bevat de verschillende scenario's die mogelijk zijn voor de vaststelling van de nieuwe omschrijvingen en een beknopt projectvoorstel voor vaststelling van de nieuwe omschrijvingen en voor vervolgonderzoek naar enkele resterende standaarden.

2 HUIDIGE OMSCHRIJVINGEN

2.1 Inleiding

Dit hoofdstuk bevat een analyse van de omschrijvingen van de functioneel toepassingsgebieden van de standaarden op de 'pas toe of leg uit'-lijst en de standaarden die nu in behandeling zijn. Eerst wordt ingegaan op de elementen waaruit de huidige omschrijvingen zijn opgebouwd. Vervolgens wordt aangegeven welke van deze elementen belangrijk zijn en welke elementen juist voor onduidelijkheid zorgen. Op basis hiervan wordt per element geadviseerd om het gebruik hiervan verplicht te stellen, toe te staan, maar niet verplicht te stellen of niet toe te staan. Als conclusie wordt een ideaaltypische syntactische structuur voorgesteld, die kan helpen om de omschrijvingen van functioneel toepassingsgebieden voor nu en in de toekomst te verduidelijken en te uniformeren.

2.2 Kenmerkende elementen

De lijst met open standaarden van het Forum Standaardisatie bevat 38 standaarden die verplicht zijn (pas toe of leg uit). Daarnaast zijn er nog 5 standaarden in behandeling voor de status 'verplicht' op de lijst met open standaarden. Bij al deze standaarden is een functioneel toepassingsgebied omschreven.

Voor alle bovenbedoelde standaarden is nagegaan welke informatie de omschrijving van hun functioneel toepassingsgebied bevat. Uit deze analyse blijkt dat de omschrijvingen zijn opgebouwd uit één of meer van de volgende 'elementen':

Element	Definitie
Functionaliteit ICT-dienst of -product	De functionaliteit waarmee een ICT-dienst of -product voorziet in een bepaalde gebruiksbehoefte. Voorbeeld (SMeF 2.0): 'De verzending van elektronische facturen [...] en de ontvangst hiervan'.
Soort ICT-dienst of -product	Een benoemde groep ICT-diensten of -producten die gemeenschappelijke kenmerken hebben (lees: voorzien in een vergelijkbare gebruiksbehoefte door een vergelijkbare functionaliteit te bieden). Voorbeeld (CMIS): 'Content Management Systemen (CMS'en) en Document Management Systemen (DMS'en)'.

Element	Definitie
Gebruiksdoel ICT-dienst of -product	Het doel waartoe gebruik wordt gemaakt van (de functionaliteit van) een ICT-dienst of -product. Voorbeeld (BWB): 'om deze [(delen van) geconsolideerde wetten en regelingen] met anderen te delen'.
Gebruikskader ICT-dienst of -product	De context waarbinnen gebruik wordt gemaakt van (de functionaliteit van) een ICT-dienst of -product. Voorbeeld (VISI): 'zowel grond- weg en waterbouw, de burger & utiliteitsbouw als de installatiebranche'.
Gebruikers ICT-dienst of -product	De organisaties of individuele eindgebruikers waardoor gebruik wordt gemaakt van (de functionaliteit van) een ICT-dienst of -product. Voorbeeld (SIKB0102): 'opgravende instanties, vondstendepots en/of archeologische registers'.
Werking standaard	De functionele of technische werking van de standaard. Voorbeeld (TLS): 'Het met behulp van certificaten beveiligen'.
Naam standaard	De volledige of verkorte naam van de standaard waarbij het functioneel toepassingsgebied is vermeld. Voorbeeld (Digikoppeling 2.0): 'DK ebMS [...], DK WUS [...], DK GB [...]' (DK staat voor Digikoppeling).
Nut standaard	Het voordeel dat toepassing van de standaard biedt ten opzichte van toepassing van geen of andere standaarden. Voorbeeld (Aquo-standaard): 'kwaliteitsverbetering van het waterbeheer'.
Uitzondering/uitsluiting	De situatie of situaties waarin gebruik van de standaard – in uitzondering op de regel – niet verplicht is. De uitzondering of uitsluiting kan zowel een ICT-dienst of -product betreffen als een standaard. Voorbeeld (WPA2 Enterprise): 'Toegang tot publieke wifi-netwerken van overheden voor gasten zonder account'.

In bijlage A worden de elementen aan de hand van voorbeelden toegelicht.

2.3 Verplichten, toestaan of niet toestaan

De aanwezigheid van een element in de omschrijving van een functioneel toepassingsgebied kan verduidelijken wanneer een standaard moet worden toegepast, maar kan het functioneel toepassingsgebied ook (onbedoeld) inperken, waardoor het niet of minder duidelijk is wanneer de standaard moet worden toegepast.

Figuur 1 laat zien welke elementen kunnen verduidelijken wanneer een standaard moet worden toegepast en welke het functioneel toepassingsgebied (onbedoeld) kunnen inperken:



Figuur 1: Beoordeling kenmerkende elementen

Het advies is om:

- elementen die verduidelijken wanneer een standaard moet worden toegepast, verplicht te stellen;
- elementen die kunnen verduidelijken wanneer een standaard moet worden toegepast, toe te staan voor zover noodzakelijk voor de verduidelijking van een functioneel toepassingsgebied, maar niet verplicht te stellen;
- elementen die het functioneel toepassingsgebied (onbedoeld) inperken, niet toe te staan.

De onderstaande tabel vat deze adviezen samen:

Element	Advies
Functionaliteit ICT-dienst of -product	Verplicht stellen
Soort ICT-dienst of -product	Toestaan, maar niet verplicht stellen
Gebruiksdoel ICT-dienst of -product	Toestaan, maar niet verplicht stellen
Gebruikskader ICT-dienst of -product	Toestaan, maar niet verplicht stellen
Gebruikers ICT-dienst of -product	Toestaan, maar niet verplicht stellen
Werking standaard	Niet toestaan

Element	Advies
Naam standaard	Niet toestaan
Nut standaard	Niet toestaan
Uitzondering/uitsluiting	Toestaan, maar niet verplicht stellen

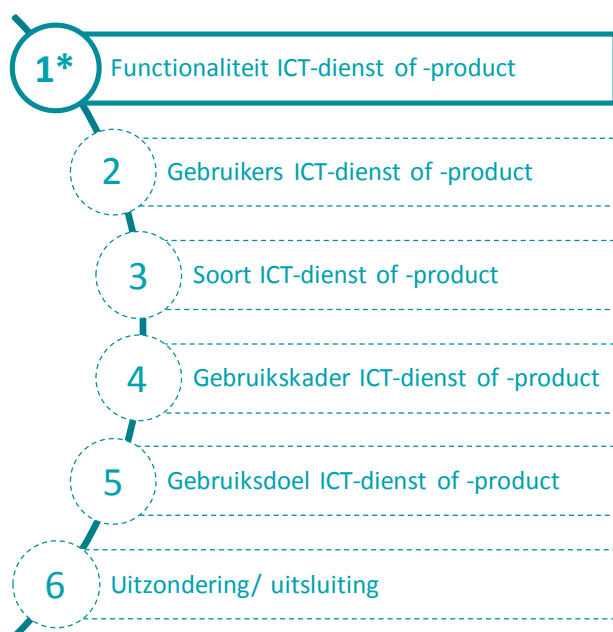
De drie elementen die volgens het advies niet zijn toegestaan, kunnen belangrijke informatie bevatten. Deze informatie hoort echter niet thuis in de omschrijving van het functioneel toepassingsgebied. De lijst met open standaarden kent hiervoor andere velden, zoals 'Nut', 'Werking' (beide onder 'Uitleg') en 'Volledige naam' (onder 'Detailinformatie'). Deze velden hebben bovendien als voordeel dat zij zonder voorafgaande procedure kunnen worden aangepast.

Procedurebegeleiders worden geadviseerd om voorzichtig te zijn met het gebruik van elementen die zijn toegestaan, maar niet verplicht zijn gesteld. De aanwezigheid van deze elementen in de omschrijving van een functioneel toepassingsgebied kan verduidelijken wanneer een standaard moet worden toegepast, maar kan het functioneel toepassingsgebied ook (onbedoeld) inperken, waardoor het niet of minder duidelijk is wanneer de standaard moet worden toegepast. Het streven is om zo duidelijk mogelijk te omschrijven wanneer een standaard moet worden toegepast, niet om alle of zoveel mogelijk elementen te gebruiken.

2.4 Ideaaltypische syntactische structuur

Gebaseerd op de bovengenoemde adviezen kan een ideaaltypische syntactische structuur worden bepaald voor de omschrijvingen van functioneel toepassingsgebieden. Zo'n structuur kan helpen om de omschrijving van functioneel toepassingsgebieden voor nu en in de toekomst te verduidelijken en te uniformeren. Figuur 2 (volgende pagina) laat een voorstel hiertoe zien.

De ideaaltypische syntactische structuur bevat het verplichte element en (voor zover noodzakelijk voor de verduidelijking van een functioneel toepassingsgebied) één of meer toegestane elementen. Elementen die niet zijn toegestaan, maken geen onderdeel uit van de ideaaltypische syntactische structuur. Vooraan staat het verplichte element: de functionaliteit waarmee een ICT-dienst of -product voorziet in een bepaalde gebruiksbehoefte. Hierdoor wordt meteen duidelijk wanneer de Rijksinstructie geldt. Met de elementen die volgen, kan nog verder worden verduidelijkt wanneer voor de betreffende standaard een ICT-dienst of ICT-product wordt aangeschaft. Het laatste element biedt een mogelijkheid om duidelijk te maken wanneer het gebruik van een standaard juist niet verplicht is.



*Invulling van het eerste veld (gemarkeerd met een *) is verplicht. Andere velden zijn optioneel. Deze mogen worden ingevuld voor zover noodzakelijk voor de verduidelijking van een functioneel toepassingsgebied.*

Figuur 2: Ideaaltypische syntactische structuur

De onderstaande tabel toont enkele mogelijke invullingen van de structuur en kan als basis worden gebruikt voor nieuwe omschrijvingen van functioneel toepassingsgebieden:

Element	Definitie
1. Functionaliteit ICT-dienst of -product	De verzending/ontvangst/publicatie/ontsluiting van gestructureerde berichten/documenten/web- of multimediacontent/metadata over ... (bijvoorbeeld 'water')
2. Gebruikers ICT-dienst of -product	met burgers/bedrijven/andere overheden die betrokken zijn bij ... (bijvoorbeeld 'het waterbeheer')
3. Soort ICT-dienst of -product	via/over/tussen websites of webapplicaties/mobiele applicaties/e-mail/openbare netwerken/informatiesystemen voor ... (bijvoorbeeld 'waterbeheer')
4. Gebruikskader ICT-dienst of -product	in het kader van ... (bijvoorbeeld 'het waterbeheer')
5. Gebruiksdoel ICT-dienst of -product	met als doel ... (bijvoorbeeld 'de kwaliteit van het waterbeheer te verbeteren'/'tijd en geld te besparen')

Element	Definitie
6. Uitzondering/uitsluiting	met uitzondering van ... (bijvoorbeeld 'werkvelden buiten de watersector').

Voor de leesbaarheid kan aan de ideaaltypische syntactische structuur nog het inleidende zinsdeel '[Naam standaard] moet worden toegepast op' worden toegevoegd.

Merk op dat verschillende elementen kunnen worden gebruikt om hetzelfde te verduidelijken. Het is niet nodig om alle elementen te gebruiken. Als in een omschrijving bijvoorbeeld wordt opgenomen dat het gaat om gegevensuitwisseling met partijen die betrokken zijn bij het waterbeheer, dan is het overbodig om in diezelfde omschrijving op te nemen dat de gegevensuitwisseling plaatsvindt in het kader van het waterbeheer en dat werkvelden buiten de watersector zijn uitgezonderd van de verplichting. In samenhang met het organisatorisch werkingsgebied moet dan duidelijk zijn welke organisatie wanneer welke standaard moet toepassen.

De ideaaltypische structuur is getoetst aan de hand van een selectie van standaarden waarvan het huidige functioneel toepassingsgebied duidelijk is omschreven en waarvan het huidige functioneel toepassingsgebied duidelijker kan worden omschreven. Deze toets heeft uitgewezen dat de ideaaltypische structuur werkbaar is en niet hoeft te worden aangepast. Zie bijlage C voor een uitwerking van de toets.

2.5 Conclusies en aanbevelingen

Bij alle verplichte standaarden is een functioneel toepassingsgebied omschreven. Een omschrijving kan zijn opgebouwd uit één of meer 'elementen'. Deze elementen kunnen verduidelijken wanneer een standaard moet worden toegepast, maar ze kunnen het functioneel toepassingsgebied ook (onbedoeld) inperken. Hierdoor is het niet of minder duidelijk wanneer de standaard moet worden toegepast.

Geadviseerd wordt om:

- elementen die verduidelijken wanneer een standaard moet worden toegepast, verplicht te stellen;
- elementen die kunnen verduidelijken wanneer een standaard moet worden toegepast, toe te staan voor zover noodzakelijk voor de verduidelijking van een functioneel toepassingsgebied, maar niet verplicht te stellen;
- elementen die het functioneel toepassingsgebied (onbedoeld) inperken, niet toe te staan.

Belangrijke informatie over bijvoorbeeld het nut van een standaard, uit de elementen die volgens het advies niet zijn toegestaan, kan beter elders worden geboden.

Gebaseerd op de bovengenoemde adviezen is een ideaaltypische syntactische structuur bepaald voor de omschrijving van functioneel toepassingsgebieden. Het Forum Standaardisatie wordt gevraagd om deze structuur goed te keuren en het gebruik hiervan onderdeel te maken van de toetsingsprocedure. Dit kan helpen om de omschrijving van functioneel toepassingsgebieden voor nu en in de toekomst te verduidelijken en te uniformeren.

Procedurebegeleiders worden geadviseerd om voorzichtig te zijn met het gebruik van elementen die zijn toegestaan, maar niet verplicht zijn gesteld. Het streven is om zo duidelijk mogelijk te omschrijven wanneer een standaard moet worden toegepast, niet om alle of zoveel mogelijk elementen te gebruiken.

3 NIEUWE OMSCHRIJVINGEN

3.1 Inleiding

Uit de analyse van de huidige omschrijvingen van de functioneel toepassingsgebieden is gebleken dat niet alle functioneel toepassingsgebieden zo zijn omschreven dat duidelijk is wanneer hiervoor een ICT-dienst of ICT-product wordt aangeschaft. Dit hoofdstuk bevat voor enkele standaarden een voorstel voor een nieuwe omschrijving. Hierbij is gebruik gemaakt van de uitgewerkte ideaaltypische syntactische structuur. Ook is rekening gehouden met reeds geldende verplichtingen en voorstellen hiertoe die specifiek van toepassing zijn op de betreffende standaarden. Eerst zal worden ingegaan op de geselecteerde standaarden en de verplichtingen die specifiek voor deze standaarden gelden.

3.2 Geselecteerde standaarden

In overleg met het Bureau Forum Standaardisatie is ervoor gekozen om die standaarden te selecteren die worden beïnvloed door de eerste tranche van de Wet GDI en door de bestuurlijke afspraken die op 2 februari 2016 zijn gemaakt in het Nationaal Beraad.

Op basis van de deze selectiecriteria, zijn de geselecteerde standaarden de volgende:

Standaard	Verplichting(en)
Digikoppeling 2.0	Wet GDI
DKIM	Wet GDI, Bestuurlijke afspraken Nationaal Beraad
DMARC	Bestuurlijke afspraken Nationaal Beraad
DNSSEC	Wet GDI
DigiToegankelijk (EN 301 549 met WCAG 2.0)	Wet GDI, Bestuurlijke afspraken Nationaal Beraad
HTTPS en HSTS	Wet GDI
SPF	Wet GDI, Bestuurlijke afspraken Nationaal Beraad
TLS	Wet GDI, Bestuurlijke afspraken Nationaal Beraad

De standaarden Digikoppeling 2.0, DKIM, DNSSEC, DigiToegankelijk (EN 301 549 met WCAG 2.0), SPF en TLS staan al op de lijst met verplichte standaarden. DMARC is op het moment van schrijven in behandeling. HTTPS en HSTS staan op de lijst met aanbevolen standaarden, maar zijn momenteel in procedure om de status te wijzigen naar 'verplicht (pas toe of leg uit)'.

3.3 Specifieke verplichtingen

In deze paragraaf wordt ingegaan op de verplichtingen die specifiek van toepassing zijn op de geselecteerde standaarden. De paragraaf is gestructureerd volgens de domeinen waartoe de geselecteerde standaarden behoren, namelijk: Document & (Web)Content, Internet & Beveiliging en Stelselstandaarden.

3.3.1 Document & (Web)Content

Binnen het domein Document & (Web)Content is één standaard geselecteerd: DigiToegankelijk (EN 301 549 met WCAG 2.0). Op deze standaard zijn de volgende verplichtingen van toepassing:

- VN-verdrag inzake de rechten van personen met een handicap (VN-verdrag Handicap);
- EU-richtlijn betreffende het plaatsen van overheidsopdrachten;
- EU-richtlijn betreffende de toegankelijkheid van de websites en mobiele applicaties van overheidsinstanties;
- Wet generieke digitale infrastructuur (Wet GDI).

VN-VERDRAG HANDICAP EN EU-RICHTLIJN INZAKE OVERHEIDSOPDRACHTEN

Het VN-verdrag Handicap en de EU-richtlijn inzake overheidsopdrachten bepalen in algemene termen dat bepaalde producten en diensten, waaronder producten en diensten op ICT-gebied, toegankelijk moeten zijn. Welke toegankelijkheidseisen precies van toepassing zijn, wordt niet in detail aangegeven. De conclusie is dat de toegankelijkheidsverplichting zoals vastgelegd in het VN-Verdrag en de EU-richtlijn te algemeen is om als basis te kunnen dienen voor de omschrijving van een functioneel toepassingsgebied, i.c. dat van DigiToegankelijk.

EU-RICHTLIJN INZAKE WEBTOEGANKELIJKHEID

De EU-richtlijn inzake webtoegankelijkheid is van toepassing op de websites en mobiele applicaties – en de content hiervan – van overheidsinstanties. In de EU-richtlijn inzake webtoegankelijkheid wordt verwezen naar EN 301 549. Hierbij zij opgemerkt dat EN 301 549 met betrekking tot mobiele applicaties verder moet worden verrijkt via een op basis van de EU-richtlijn aangenomen technische specificatie.

De EU-richtlijn inzake webtoegankelijkheid is voldoende specifiek geformuleerd om te kunnen dienen voor de omschrijving van het functioneel toepassingsgebied van DigiToegankelijk. Het functioneel toepassingsgebied van DigiToegankelijk dient dan ook op de EU-richtlijn te worden afgestemd. Tot oplevering van de eerder genoemde technische specificaties, kan toepassing van DigiToegankelijk op mobiele applicaties niet verplicht worden gesteld op de lijst met open standaarden.

WET GDI

De EU-richtlijn inzake webtoegankelijkheid zal naar verwachting worden omgezet via de Wet GDI. Het functioneel toepassingsgebied van DigiToegankelijk wordt bepaald door de EU-richtlijn. In tegenstelling tot andere standaarden, is hier niet of nauwelijks eigen invloed op.

Artikel 2 lid 2 van het wetsvoorstel GDI bepaalt dat bij algemene maatregel van bestuur (AMvB) open standaarden kunnen worden aangewezen, die overheden dienen te hanteren in het elektronisch verkeer met andere overheden, met burgers en met bedrijven. Uit de memorie van toelichting bij de Wet GDI blijkt dat de regering – in verband met de EU-richtlijn betreffende de toegankelijkheid van de websites en mobiele applicaties van overheidsinstanties – voornemens is om DigiToegankelijk aan te wijzen als verplicht toe te passen standaard.

Volgens de memorie van toelichting bij de Wet GDI zal een bij AMvB verplichte standaard van de lijst met open standaarden worden verwijderd. Er kunnen redenen zijn om dit niet te doen, bijvoorbeeld omdat het toepassingsbereik van de AMvB beperkter is dan het functioneel toepassingsgebied of het organisatorisch werkingsgebied van de lijst met open standaarden. Hoofdstuk 4 bevat hiertoe een procesvoorstel.

3.3.2 Internet & Beveiliging

Binnen het domein Internet & Beveiliging zijn de volgende standaarden geselecteerd:

- DKIM
- DMARC
- DNSSEC
- HTTPS en HSTS
- SPF
- TLS

Op deze standaarden zijn één of meer van de volgende verplichtingen van toepassing:

- Wet generieke digitale infrastructuur (Wet GDI)
- Regeling voorzieningen GDI
- Besluit elektronische dienstverlening burgerlijke stand
- Beleidsregels van de Autoriteit Persoonsgegevens
- Bestuurlijke afspraken van het Nationaal Beraad
- Sectorale baselines informatiebeveiliging
- Adviezen van het NCSC
- Norm ICT-beveiligingsassessments DigiD
- Afsprakenstelsel Elektronische Toegangsdiensten
- Lijst met open standaarden van het Forum Standaardisatie

In het onderstaande wordt op deze verplichtingen één voor één ingegaan, waarbij per verplichting wordt aangegeven op welke van de geselecteerde standaarden deze van toepassing is en of deze invloed heeft op de omschrijvingen van de functioneel toepassingsgebieden van de betreffende standaarden of niet.

WET GDI

Uit de memorie van toelichting bij de Wet GDI blijkt dat de regering voornemens is om DKIM, DNSSEC, SPF en TLS aan te wijzen als verplicht toe te passen standaarden. De minister van

Binnenlandse Zaken en Koninkrijksrelaties heeft bovendien aangegeven alle overheidssites wettelijk te willen verplichten om een beveiligde internetverbinding, via de HTTPS-standaard, te gebruiken. Het voornemen is om ook HTTPS bij AMvB aan te wijzen. In de AMvB zal het toepassingsbereik van de standaarden worden omschreven. De memorie van toelichting bevat hiervoor al enige aanknopingspunten. De functioneel toepassingsgebieden van DKIM, DNSSEC, HTTPS en HSTS, SPF en TLS zullen hierop moeten worden afgestemd of vice versa. Hoofdstuk 4 bevat hiertoe een procesvoorstel.

REGELING VOORZIENINGEN GDI

In de Regeling voorzieningen GDI zijn regels opgenomen met betrekking tot de werking, beveiliging en betrouwbaarheid van voorzieningen voor elektronisch berichtenverkeer en informatieverschaffing (MijnOverheid), voor elektronische authenticatie (DigiD, BSN-koppelregister) en voor elektronische registratie van machtigingen (DigiD Machtigen). In de regeling wordt onder meer verwezen naar de open normen en standaarden op de 'pas-toe-of-leg-uit-lijst' van het Forum Standaardisatie. Specifieke standaarden worden in de regeling niet genoemd. De conclusie is dat de regeling te algemeen is geformuleerd om als basis te kunnen dienen voor de omschrijving van een functioneel toepassingsgebied, i.c. dat van de informatieveiligheidsstandaarden.

BESLUIT ELEKTRONISCHE DIENSTVERLENING BURGERLIJKE STAND

Het Besluit elektronische dienstverlening burgerlijke stand stelt enkele randvoorwaarden aan de elektronische dienstverlening door de burgerlijke stand, waaronder dat de volgende open standaarden worden toegepast:

- Webrichtlijnen⁷ om ervoor te zorgen dat een overheidswebsite toegankelijk is voor iedere burger;
- TLS in de vorm van https om de authenticiteit van de website te kunnen bepalen en de gegevensuitwisseling te versleutelen;
- DNSSEC voor domeinnaambeveiliging die «bewegwijzeringsfraude» op internet tegengaat;
- Digikoppeling voor veilige gegevensuitwisseling met andere overheden, waaronder basisregistraties.

De randvoorwaarden gelden alleen voor bepaalde systemen die de burgerlijke stand gebruikt voor gegevensverwerking. Het toepassingsbereik van het Besluit elektronische dienstverlening burgerlijke stand is dus beperkter dan het functioneel toepassingsgebied (en het organisatorisch werkingsgebied) van de standaarden op de lijst met open standaarden. De formulering van de randvoorwaarden kan echter wel worden gebruikt als basis voor de omschrijvingen van de functioneel toepassingsgebieden van de betreffende standaarden.

⁷ De Webrichtlijnen zijn vervangen door DigiToegankelijk (EN 301 549 met WCAG 2.0).

BELEIDSREGELS AUTORITEIT PERSOONSGEGEVENS

De Autoriteit Persoonsgegevens zet in beleidsregels (voorheen: richtsnoeren) uiteen welke uitleg van de wettelijke normen de autoriteit hanteert bij de uitoefening van haar bevoegdheden. In 2013 zijn de 'Richtsnoeren beveiliging van persoonsgegevens' gepubliceerd. Deze richtsnoeren leggen uit hoe de autoriteit bij het onderzoeken en beoordelen van de beveiliging van persoonsgegevens de beveiligingsnormen uit de Wet bescherming persoonsgegevens (Wbp) toepast.

Artikel 13 van de Wbp eist dat bedrijven en overheden die persoonsgegevens verwerken, 'passende technische en organisatorische maatregelen' nemen om persoonsgegevens te beveiligen. De Autoriteit Persoonsgegevens beschouwt het gebruik van standaarden als een randvoorwaarde om tot passende maatregelen te komen zoals de wet die voorschrijft.

De Autoriteit Persoonsgegevens geeft in de Richtsnoeren beveiliging van persoonsgegevens concrete voorbeelden van standaarden, maar noemt geen van de geselecteerde standaarden direct. De richtsnoeren zijn daarom niet geschikt om als basis te dienen voor de omschrijving van de functioneel toepassingsgebieden van de geselecteerde standaarden.

BESTUURLIJKE AFSPRAKEN NATIONAAL BERAAD

In het Nationaal Beraad van 2 februari 2016 zijn aanvullende resultaatafspraken gemaakt over de adoptie van de informatieveiligheidsstandaarden TLS, DNSSEC, DMARC, SPF en DKIM. Het afgesproken streefbeeld is dat deze standaarden eind 2017 overal – waar van toepassing – binnen de overheid zijn geïmplementeerd. De omschrijvingen van de functioneel toepassingsgebieden van TLS, DNSSEC, DMARC, SPF en DKIM verschillen van de formuleringen van de resultaatafspraken en zullen hier inhoudelijk op moeten worden afgestemd.

SECTORALE BASELINES INFORMATIEBEVEILIGING

De Nederlandse overheid heeft haar eigen kaders voor informatiebeveiliging afgeleid van de NEN-ISO/IEC 27001 en 27002 normen. Dit zijn de sectorale baselines informatiebeveiliging, oftewel de Baseline Informatiebeveiliging Rijksdienst (BIR), de Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG), de Baseline Informatiebeveiliging Waterschappen (BIWA) en de Interprovinciale Baseline Informatiebeveiliging (IBI). Het voornemen is om tot een baseline informatiebeveiliging voor de gehele overheid (BIO) te komen, die de huidige baselines binnen de overheid vervangt. De sectorale baselines informatiebeveiliging maken over het algemeen onderscheid tussen een strategisch, tactisch en operationeel niveau, met afzonderlijke documenten voor ieder niveau. Alleen in sommige documenten op operationeel niveau worden, in dit verband relevante, standaarden genoemd. Deze documenten zijn geschikt om als basis te dienen voor de omschrijvingen van de functioneel toepassingsgebieden van de betreffende standaarden. De andere documenten niet.

ADVIEZEN NCSC

Het NCSC publiceert regelmatig factsheets, whitepapers en dergelijke om kennis te verspreiden. In dit verband relevante voorbeelden zijn de ICT-beveiligingsrichtlijnen voor Transport Layer Security (TLS), de ICT-beveiligingsrichtlijnen voor Webapplicaties en de Beveiligingsrichtlijnen voor mobiele apparaten. Deze richtlijnen zijn formeel aanbevelingen, maar wel met grote bekendheid en gezag. Andere relevante voorbeelden zijn de factsheet 'Bescherm domeinnamen tegen phishing' en de factsheet 'HTTPS kan een stuk veiliger'. In deze documenten wordt ingegaan op alle geselecteerde informatieveiligheidsstandaarden: DKIM, DMARC, DNSSEC, HTTPS en HSTS, SPF en TLS. De documenten van het NCSC kunnen worden gebruikt als basis voor de omschrijving van de functioneel toepassingsgebieden van de betreffende standaarden, maar gaan meer in op de werking van de standaard.

NORM ICT-BEVEILIGINGSASSESSMENTS DIGID

De Norm ICT-beveiligingsassessments DigiD is een afgeleide van de beveiligingsrichtlijnen voor webapplicaties van het NCSC.

Het NCSC heeft de beveiligingsrichtlijnen voor webapplicaties in 2015 vernieuwd. Op basis daarvan is in 2016 een nieuwe versie van het normenkader, versie 2.0, vastgesteld⁸. De huidige versie van het normenkader, versie 1.0, is tot 1 juli 2017 van toepassing. Tussen 1 juli 2017 en 1 november 2017 kan worden gekozen voor de huidige versie of de nieuwe versie. Na 1 november 2017 zijn organisaties verplicht om nieuwe aansluitingen te toetsen tegen het nieuwe normenkader.

In de huidige versie wordt HTTPS als enige standaard expliciet genoemd, in verband met versleutelde verbindingen. In de nieuwe versie worden geen standaarden bij naam genoemd. Wel zijn hierin richtlijnen U/WA.05 en U/NW.06 uit de 'ICT-beveiligingsrichtlijnen voor webapplicaties' van NCSC verplicht gesteld. De Handreiking bij DigiD-assessments V2.0⁹ van NOREA noemt de HTTPS configuratie en de TLS configuratie als aandachtspunten bij richtlijn U/WA.05. Als uitwerking van richtlijn U/NW.06, stelt de handreiking van NOREA het gebruik van DNSSEC verplicht.

De Norm ICT-beveiligingsassessments DigiD alleen, is niet geschikt om als basis te dienen voor de omschrijvingen van het toepassingsgebied van de informatieveiligheidsstandaarden. De hieraan gerelateerde documenten 'ICT-beveiligingsrichtlijnen voor webapplicaties' van NCSC en 'Handreiking bij DigiD-assessments V2.0' van NOREA kunnen wel als basis dienen.

⁸ 20161215_norm_V2_ict-beveiligingsassessments_digid.pdf

⁹ <https://www.norea.nl/download/?id=2562>

AFSPRAKENSTELSEL ELEKTRONISCHE TOEGANGSDIENSTEN

Het Afsprakenstelsel Elektronische Toegangsdiensden is een set van technische, functionele, juridische en organisatorische afspraken op basis waarvan de elektronische toegangsdiensden eHerkenning en Idensys worden geleverd. Het afsprakenstelsel beschrijft onder meer de eisen die van toepassing zijn op de genomen beveiligingsmaatregelen, waaronder DNSSEC en TLS. Dit kan worden gebruikt om het functioneel toepassingsgebied van deze standaarden te concretiseren.

LIJST MET OPEN STANDAARDEN

HTTPS en HSTS staan op de lijst met aanbevolen standaarden, maar zijn momenteel in procedure om de status te wijzigen naar 'verplicht (pas toe of leg uit)'. Hierbij is het functioneel toepassingsgebied iets gewijzigd. Het gewijzigde functioneel toepassingsgebied is nog niet vastgesteld, maar hier kan bij de nieuwe omschrijving al wel rekening mee te worden gehouden.

3.3.3 Stelselstandaarden

Binnen het domein Stelselstandaarden is één standaard geselecteerd: Digikoppeling 2.0. Op deze standaard zijn de volgende verplichtingen van toepassing:

- Lijst met open standaarden van het Forum Standaardisatie;
- Landelijke voorzieningen.

LIJST MET OPEN STANDAARDEN

Digikoppeling 3.0 is aangemeld en in procedure genomen voor opname op de 'pas toe of leg uit'-lijst, maar zal worden teruggetrokken. Het functioneel toepassingsgebied van Digikoppeling 3.0 is al wel in concept omschreven. De omschrijving van het functioneel toepassingsgebied van Digikoppeling 3.0 is anders dan dat van Digikoppeling 2.0. Bij herformulering kan hier rekening worden gehouden.

LANDELIJKE VOORZIENINGEN

Steeds meer landelijke voorzieningen maken (verplicht) gebruik van Digikoppeling. Het gaat hier om voorzieningen die onderdeel zijn van de GDI, waaronder de basisregistraties, maar ook om andere voorzieningen die sectoroverstijgend zijn. Zo loopt de aansluiting op de Landelijke Voorziening WOZ via Digikoppeling en ook de aansluitingen op Omgevingsloket online (OLO) en de Collectieve Opdracht Routeer Voorziening (CORV). Deze toepassingen van Digikoppeling kunnen worden gebruikt om het functioneel toepassingsgebied te concretiseren.

3.4 Nieuwe omschrijvingen

Hieronder wordt voor enkele geselecteerde standaarden een voorstel gedaan voor een nieuwe omschrijving. Hierbij is gebruik gemaakt van de eerder uitgewerkte ideaaltypische syntactische structuur en is rekening gehouden met de verplichtingen die specifiek voor deze standaarden gelden. De paragraaf is gestructureerd volgens de domeinen waartoe de geselecteerde standaarden behoren: Document & (Web)Content, Internet & Beveiliging en Stelselstandaarden.

3.4.1 Document & (Web)Content

Binnen het domein Document & (Web)Content is één standaard geselecteerd: DigiToegankelijk (EN 301 549 met WCAG 2.0). De onderstaande tabel toont hoe het functioneel toepassingsgebied van deze standaard momenteel is omschreven en wat de voorgestelde nieuwe omschrijving is.

Huidige omschrijving	Nieuwe omschrijving
EN 301 549 is van toepassing op webgebaseerde informatie-, interactie-, transactie- en participatiediensten.	DigiToegankelijk (EN 301 549 met WCAG 2.0) moet worden toegepast op de levering van informatie-, interactie-, transactie- en participatiediensten aan burgers, bedrijven en andere overheden via websites of webapplicaties.

Vanwege de ideaaltypische syntactische structuur is 'EN 301 549 is van toepassing op' herschreven. Verder is 'webgebaseerde informatie-, interactie-, transactie- en participatiediensten' uiteengehaald in 'de levering van informatie-, interactie-, transactie- en participatiediensten (1. Functionaliteit ICT-dienst of -product) via websites of webapplicaties (3. Soort ICT-dienst of -product)' en is toegevoegd dat de diensten worden geleverd aan burgers, bedrijven en andere overheden (2. Gebruikers ICT-dienst of -product).

3.4.2 Internet & Beveiliging

Binnen het domein Internet & Beveiliging zijn de volgende standaarden geselecteerd:

- DKIM
- DMARC
- DNSSEC
- HTTPS en HSTS
- SPF
- TLS

DKIM

De onderstaande tabel toont hoe het functioneel toepassingsgebied van DKIM momenteel is omschreven en wat de voorgestelde nieuwe omschrijving is.

Huidige omschrijving	Nieuwe omschrijving
Het faciliteren van het vaststellen van organisatorische herkomst voor e-mail afkomstig van overheidsdomeinen, als deze over een onbeveiligde, publieke internetverbinding wordt verstuurd wanneer verdere authenticatie ontbreekt.	DKIM moet worden toegepast op alle overheidsdomeinnamen, inclusief die waarvan niet wordt gemaild, én op alle mailsystemen waarmee de overheid e-mail verstuurt of ontvangt.

Vanwege de ideaaltypische syntactische structuur is het inleidende zinsdeel 'DKIM moet worden toegepast op' toegevoegd. Verder is 'Het faciliteren van het vaststellen van organisatorische herkomst voor' komen te vervallen, vanwege het advies om de functionele of technische werking van de standaard niet toe te staan. In lijn met de resultaatspraak die in het Nationaal Beraad van 2 februari 2016 is gemaakt over de adoptie van DKIM, DMARC en SPF, is het toepassingsgebied verbreed van het versturen van e-mail tot alle overheidsdomeinnamen (3. Soort ICT-dienst of -product) of deze nu wel of niet gebruik maken van mail (1. Functionaliteit ICT-dienst of -product). Om volledig te zijn, is 'op alle mailsystemen (3. Soort ICT-dienst of -product) waarmee de overheid e-mail verstuurt of ontvangt' (1. Functionaliteit ICT-dienst of -product) toegevoegd.

DMARC

De onderstaande tabel toont hoe het functioneel toepassingsgebied van DMARC momenteel is omschreven en wat de voorgestelde nieuwe omschrijving is.

Huidige omschrijving	Nieuwe omschrijving
Het instellen van beleid voor alle domeinnamen, waarvan de overheid de houder is, om betrouwbare e-mailcommunicatie met burgers, bedrijven en (semi)overheidsorganisaties te bevorderen, alsmede de bescherming van de overheid zelf tegen e-mail van ongeauthenticeerde afzenders te bevorderen.	DMARC moet worden toegepast op alle overheidsdomeinnamen, inclusief die waarvan niet wordt gemaild, én op alle mailsystemen waarmee de overheid e-mail verstuurt of ontvangt.

Vanwege de ideaaltypische syntactische structuur is het inleidende zinsdeel 'DMARC moet worden toegepast op' toegevoegd. Verder zijn 'Het instellen van beleid voor', 'om betrouwbare', 'te bevorderen, alsmede de bescherming van de overheid zelf tegen e-mail van ongeauthenticeerde [sic] afzenders te bevorderen' komen te vervallen, vanwege het advies om de functionele of technische werking van de standaard niet toe te staan. Wat dan overblijft is een functioneel toepassingsgebied dat iets herschreven moet worden om dit tekstueel kloppend te maken. Inhoudelijk komt dit vrijwel overeen met dat van DKIM, wat juist is. De nieuwe omschrijving is gelijk aan die van DKIM.

DNSSEC

De onderstaande tabel toont hoe het functioneel toepassingsgebied van DNSSEC momenteel is omschreven en wat de voorgestelde nieuwe omschrijving is.

Huidige omschrijving	Nieuwe omschrijving
Het registreren en in DNS publiceren van internet-domeinnamen ('signing'). De registratieverplichting geldt enkel indien 'signed domain names' bij een registerhouder van een top-level domein (zoals SIDN voor .NL) geautomatiseerd aangevraagd kunnen worden;	DNSSEC moet worden toegepast op alle overheidsdomeinnamen én op alle direct aan internet gekoppelde systemen die domeinnamen opvragen.
Het vertalen van domeinnamen naar internetadressen en vice versa ('validation enabled resolving'). Validatie is niet verplicht voor systemen die niet direct aan het publieke internet gekoppeld zijn (bijvoorbeeld clients/werkplekken binnen een LAN en interne DNS-systemen).	

Vanwege de ideaaltypische syntactische structuur is het inleidende zinsdeel 'DNSSEC moet worden toegepast op' toegevoegd. Verder is een groot deel van de omschrijving komen te vervallen, vanwege het advies om de functionele of technische werking van de standaard niet toe te staan. Wat is overgebleven van de omschrijving is, zij het in andere bewoordingen, gestructureerd volgens de ideaaltypische syntactische structuur.

HTTPS EN HSTS

De onderstaande tabel toont hoe het functioneel toepassingsgebied van HTTPS en HSTS momenteel is omschreven en wat de voorgestelde nieuwe omschrijving is.

Huidige omschrijving	Nieuwe omschrijving
Beveiligde uitwisseling van gegevens via het web	HTTPS EN HSTS moeten worden toegepast op de communicatie tussen clients (zoals webbrowsers) en servers voor alle via internet benaderbare overheidswebsites en -webservices.

Vanwege de ideaaltypische syntactische structuur is het inleidende zinsdeel 'HTTPS EN HSTS moeten worden toegepast op' toegevoegd. Verder is 'Beveiligde' komen te vervallen, vanwege het advies om de functionele of technische werking van de standaard niet toe te staan. Ook is de omschrijving gepreciseerd met behulp van elementen uit de omschrijving van het functioneel toepassingsgebied zoals dat is voorgesteld in het expertadvies voor HTTPS en HSTS dat op dit moment ter consultatie ligt. De voorgestelde omschrijving is ingegeven door het voornemen van de minister van Binnenlandse Zaken en Koninkrijksrelaties om alle overheidssites wettelijk te verplichten om een beveiligde internetverbinding, via de HTTPS-standaard, te gebruiken.

SPF

De onderstaande tabel toont hoe het functioneel toepassingsgebied van SPF momenteel is omschreven en wat de voorgestelde nieuwe omschrijving is.

Huidige omschrijving	Nieuwe omschrijving
Het controleren of een e-mailserver gerechtigd is om namens een domeinnaam e-mail te mogen verzenden	SPF moet worden toegepast op alle overheidsdomeinnamen, inclusief die waarvan niet wordt gemaild, én op alle mailsystemen waarmee de overheid e-mail verstuurt of ontvangt.

Vanwege de ideaaltypische syntactische structuur is het inleidende zinsdeel 'SPF moet worden toegepast op' toegevoegd. Verder is 'Het controleren of ... gerechtigd is om' komen te vervallen, vanwege het advies om de functionele of technische werking van de standaard niet toe te staan. Wat dan overblijft moet – net als bij DMARC – iets worden herschreven om dit tekstueel kloppend te maken. Inhoudelijk komt dit vrijwel overeen met het functioneel toepassingsgebied van DKIM en DMARC, wat juist is. De nieuwe omschrijving is gelijk aan die van DKIM en DMARC.

TLS

De onderstaande tabel toont hoe het functioneel toepassingsgebied van TLS momenteel is omschreven en wat de voorgestelde nieuwe omschrijving is.

Huidige omschrijving	Nieuwe omschrijving
Het met behulp van certificaten beveiligen van de verbinding (op de transportlaag) tussen client- en serversystemen of tussen serversystemen onderling, voor zover deze gerealiseerd wordt met internettechnologie.	TLS moet worden toegepast op de uitwisseling van gegevens tussen clients en servers en tussen servers onderling voor zover deze uitwisseling over internet plaatsvindt.

Vanwege de ideaaltypische syntactische structuur is het inleidende zinsdeel 'TLS moet worden toegepast op' toegevoegd. Verder is de tekst over de certificaten en transportlaag komen te vervallen, vanwege het advies om de functionele of technische werking van de standaard niet toe te staan. Het deel met internettechnologie is – zij het in andere bewoordingen – behouden, omdat dit verduidelijkt om wat voor soort ICT-dienst of -product het gaat (internetverbindingen). Het functioneel toepassingsgebied is nader gepreciseerd door in de omschrijving op te nemen waarvoor de internetverbindingen worden gebruikt, namelijk de uitwisseling van gegevens (1. Functionaliteit ICT-dienst of -product).

3.4.3 Stelselstandaarden

Binnen het domein Stelselstandaarden is Digikoppeling geselecteerd. De onderstaande tabel toont hoe het functioneel toepassingsgebied van deze standaard momenteel is omschreven en wat de voorgestelde nieuwe omschrijving is.

Huidige omschrijving	Nieuwe omschrijving
Geautomatiseerde gegevensuitwisseling tussen informatiesystemen voor sectoroverstijgend berichtenverkeer, op basis van drie koppelvlakstandaarden: • DK ebMS standaard voor meldingen tussen informatiesystemen • DK WUS standaard voor de bevraging van informatiesystemen • DK GB standaard voor de uitwisseling van grote berichten	Digikoppeling moet worden toegepast op alle digitale gegevensuitwisseling met behulp van gestructureerde berichten die plaatsvindt met voorzieningen die onderdeel zijn van de GDI, waaronder de basisregistraties, of die sectoroverstijgend is. Bij dit laatste kan worden gedacht aan de uitwisseling van berichten tussen bijvoorbeeld een gemeente en een uitvoeringsorganisatie. Uitgezonderd is de verplichting tot het gebruik van NEN3610 (geo-standaarden) en uitgezonderd zijn de gevallen waarin de aanbieder van gegevens vaststelt dat geen noodzaak bestaat om de afnemer van de gegevens te authenticeren.

Vanwege de ideaaltypische syntactische structuur is het inleidende zinsdeel 'Digikoppeling moet worden toegepast op' toegevoegd. Verder is het deel met de koppelvlakstandaarden DK ebMS, DK WUS en DK GB (DK staat voor Digikoppeling) komen te vervallen, vanwege het advies om de volledige of verkorte naam van de standaard waarbij het functioneel toepassingsgebied is vermeld, niet toe te staan. Het overblijvende toepassingsgebied is gepreciseerd op basis van het functioneel toepassingsgebied zoals dat is voorgesteld voor Digikoppeling 3.0. Om duidelijk te maken wat wordt bedoeld met digitale gegevensuitwisseling die sectoroverstijgend is, is hieraan nog toegevoegd: 'Bij dit laatste kan worden gedacht aan de uitwisseling van berichten tussen bijvoorbeeld een gemeente en een uitvoeringsorganisatie'.

3.5 Conclusies en aanbevelingen

Naast de behoefte aan meer duidelijkheid, vormen de Wet GDI, de resultaatafspraken die op 2 februari 2016 zijn gemaakt in het Nationaal Beraad, en enkele andere verplichtingen, zoals de adviezen van het NCSC, aanleiding om eens goed naar de omschrijvingen van de functioneel toepassingsgebieden te kijken.

Gebruik makend van de eerder uitgewerkte ideaaltypische syntactische structuur en rekening houdend met de verplichtingen die specifiek voor deze standaarden gelden, is voor

DigiToegankelijk (EN 301 549 met WCAG 2.0), DKIM, DMARC, DNSSEC, HTTPS en HSTS, SPF, TLS en Digikoppeling 2.0 een voorstel gedaan voor een nieuwe omschrijving.

Het Forum Standaardisatie wordt gevraagd om de nieuwe omschrijvingen goed te keuren dan wel vast te stellen. Hoofdstuk 4 bevat hiertoe een procesvoorstel.

4 VERVOLGAANPAK

4.1 Inleiding

Dit hoofdstuk bevat een voorstel voor de vervolgaanpak van de verduidelijking van de functioneel toepassingsgebieden. Allereerst wordt ingegaan op de verschillende scenario's die mogelijk zijn voor de vaststelling van de nieuwe omschrijvingen. Vervolgens komen de standaarden aan bod waarvan wordt geadviseerd om ook de functioneel toepassingsgebieden opnieuw te omschrijven. Het hoofdstuk wordt afgesloten met een beknopt projectvoorstel voor vaststelling van de nieuwe omschrijvingen en vervolgonderzoek naar de resterende standaarden.

4.2 Scenario's

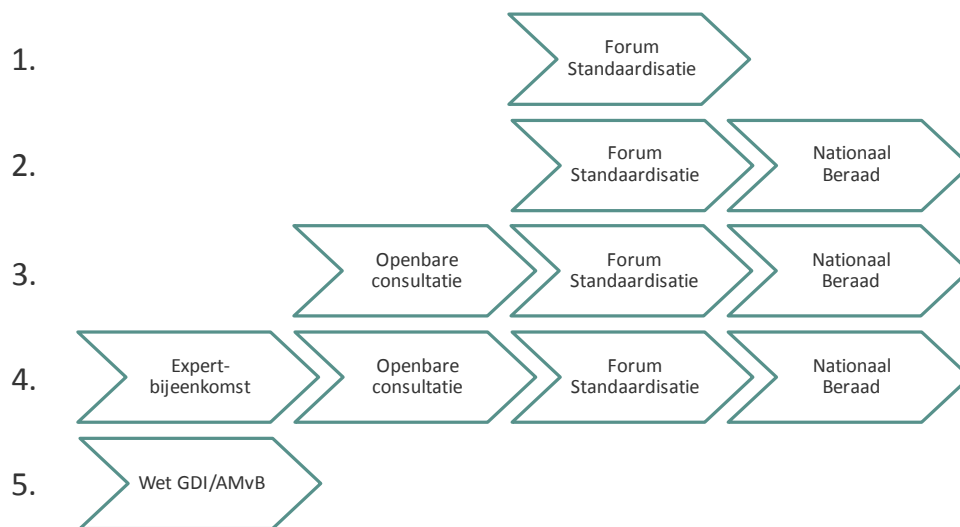
De nieuwe omschrijvingen van de functioneel toepassingsgebieden kunnen – net als een standaard in procedure – verschillende stadia doorlopen: van expertonderzoek, via openbare consultatie en advisering door de stuurgroep Open Standaarden aan het Forum Standaardisatie tot aan officiële vaststelling door het Nationaal Beraad. De gehele procedure doorlopen is voor één wijziging wel een zeer uitgebreide aanpak.

Welke stadia een nieuwe omschrijving zal doorlopen, is afhankelijk van het verschil met de huidige omschrijving. Als dit verschil klein is, dan kan vaststelling door het Forum Standaardisatie volstaan. Is het verschil groot, dan zullen al gauw een openbare consultatie en vaststelling door het Nationaal Beraad nodig zijn. Een mogelijkheid is ook dat een nieuwe omschrijving wordt overgedragen aan het traject om standaarden bij AMvB voor te schrijven (Wet GDI). Dit kan direct, maar ook na bijvoorbeeld openbare consultatie of vaststelling door het Nationaal Beraad.

Figuur 3 (volgende pagina) toont de verschillende scenario's die mogelijk zijn voor de vaststelling van de nieuwe omschrijvingen.

De nieuwe omschrijving van DigiToegankelijk (EN 301 549 met WCAG 2.0) verschilt niet veel van de huidige omschrijving en blijft inhoudelijk hetzelfde. Geadviseerd wordt om deze omschrijving door het Forum Standaardisatie vast te laten stellen, zonder extra expertbijeenkomst en openbare consultatie.

De verschillen tussen de nieuwe omschrijvingen van de informatieveiligheidsstandaarden (DKIM, DMARC, DNSSEC, HTTPS en HSTS, SPF en TLS) en de huidige omschrijvingen zijn relatief groot. Vanwege hun onderlinge samenhang, wordt geadviseerd om deze omschrijvingen als één pakket ter consultatie voor te leggen en, na goedkeuring door het Forum Standaardisatie, vast te laten stellen door het Nationaal Beraad. Daarnaast is het aan te bevelen om ook de oude expertgroep in te lichten. Zodra het traject om standaarden bij AMvB voor te schrijven (Wet GDI) loopt, kunnen de vastgestelde omschrijvingen als input aan dit traject worden meegegeven.



Figuur 3: Scenario's voor vaststelling nieuwe omschrijvingen

De nieuwe omschrijving van het functioneel toepassingsgebied van Digikoppeling 2.0 is nagenoeg onveranderd overgenomen van de omschrijving van Digikoppeling 3.0. Digikoppeling 3.0 is in consultatie geweest, maar zal worden teruggetrokken. Geadviseerd wordt om de nieuwe omschrijving voor te leggen aan de deelnemers aan de consultatie van Digikoppeling 3.0 en de omschrijving, na goedkeuring door het Forum Standaardisatie, vast te laten stellen door het Nationaal Beraad.

Onderstaande tabel vat de geadviseerde scenario's samen:

Standaarden	Vaststelling
DigiToegankelijk (EN 301 549 met WCAG 2.0)	Forum Standaardisatie
DKIM, DMARC, DNSSEC, HTTPS en HSTS, SPF en TLS	Openbare consultatie, Forum Standaardisatie, Nationaal Beraad
Digikoppeling	Niet-openbare consultatie, Forum Standaardisatie, Nationaal Beraad

4.3 Resterende standaarden

De lijst met open standaarden van het Forum Standaardisatie bevat 38 standaarden die verplicht zijn krachtens het 'pas toe of leg uit'-beleid. Daarnaast zijn er nog 5 standaarden in behandeling voor de status 'verplicht (pas toe of leg uit)' op de lijst met open standaarden. Het functioneel toepassingsgebied van 8 van deze standaarden is als onderdeel van dit onderzoek opnieuw omschreven. De resterende 35 standaarden zijn ongemoeid gelaten, terwijl de functioneel toepassingsgebieden van deze standaarden niet allemaal even duidelijk zijn omschreven.

Op basis van de elementen waaruit de omschrijvingen kunnen zijn opgebouwd en de adviezen die hierover zijn uitgebracht, is een rekenmodel gemaakt waarmee op een schaal van 1 tot en met 5 uitspraken kunnen worden gedaan over de duidelijkheid van de omschrijvingen. Een score van 5 staat voor de meest duidelijke omschrijvingen. Een score van 1 staat voor de minst duidelijke omschrijvingen.

Het rekenmodel houdt rekening met de aan- of afwezigheid van de onderscheiden elementen (zie paragraaf 2.2) en de adviezen om deze te verplichten, toe te staan of niet toe te staan (paragraaf 2.3). De aanwezigheid van elementen die verduidelijken wanneer een standaard moet worden toegepast, levert 4 punten op. De aanwezigheid van elementen die kunnen verduidelijken wanneer een standaard moet worden toegepast levert 1 punt op. De aanwezigheid van elementen die het functioneel toepassingsgebied (onbedoeld) inperken levert 1 punt aftrek op. Scores kunnen niet hoger zijn dan 5 en niet lager dan 1. NB. Het model houdt geen rekening met de duidelijkheid waarmee de individuele elementen zijn omschreven.

Rekenvoorbeeld

Aquo-standaard: Uitwisselen van uniforme (Werking, -1) gegevens over water (Functionaliteit, +4) tussen partijen die betrokken zijn bij het waterbeheer (Gebruikers, +1) voor de kwaliteitsverbetering van het waterbeheer (Nut, -1) (Score = 3).

De onderstaande tabel toont alle standaarden met een score die lager is dan 4 en waarvan het functioneel toepassingsgebied niet al opnieuw in bovenstaande advies is omschreven:

Standaard	Score	Domein
NEN-ISO/IEC 27001	1	Internet & Beveiliging
NEN-ISO/IEC 27002	1	Internet & Beveiliging
STARTTLS en DANE	1	Internet & Beveiliging
WPA2 Enterprise	1	Internet & Beveiliging
Oauth	3	Internet & Beveiliging
SAML	3	Internet & Beveiliging
Aquo-standaard	3	Water/Bodem

Geadviseerd wordt om ook de functioneel toepassingsgebieden van deze standaarden opnieuw te omschrijven. Zie bijlage B voor de scores van alle verplichte standaarden.

4.4 Aanpak

De vervolgaanpak kan worden uitgevoerd in vijf stappen. De eerste twee stappen zijn alleen van toepassing op vervolgonderzoek naar de resterende standaarden. Voor DigiToegankelijk (EN 301 549 met WCAG 2.0), de informatieveiligheidsstandaarden (DKIM, DMARC, DNSSEC, HTTPS en HSTS, SPF en TLS) en Digikoppeling 2.0 zijn deze stappen al gezet.

1. ANALYSEREN SPECIFIEKE VERPLICHTINGEN

Op de in paragraaf 4.3 genoemde standaarden kunnen verplichtingen van toepassing zijn die invloed hebben op de omschrijvingen van de functioneel toepassingsgebieden. In deze stap worden deze verplichtingen geïnventariseerd en geanalyseerd.

2. OPSTELLEN NIEUWE OMSCHRIJVINGEN

In deze stap wordt voor de geselecteerde standaarden een voorstel gedaan voor een nieuwe omschrijving. Hierbij zal gebruik worden gemaakt van de eerder uitgewerkte ideaaltypische syntactische structuur en rekening worden gehouden met de verplichtingen die specifiek voor deze standaarden gelden.

3. UITVOEREN OPENBARE CONSULTATIE

Om ervoor te zorgen dat belanghebbenden kunnen reageren, worden de nieuwe omschrijvingen van de functioneel toepassingsgebieden onderwerp van een openbare consultatie. Na afloop hiervan, worden de reacties verwerkt in de omschrijvingen en worden de omschrijvingen voor advies voorgelegd aan de stuurgroep Open Standaarden.

4. GOEDKEUREN NIEUWE OMSCHRIJVINGEN

Na enkele voorziene laatste iteraties worden de definitieve omschrijvingen opgeleverd en ter goedkeuring voorgelegd aan het Forum Standaardisatie.

5. VASTSTELLEN NIEUWE OMSCHRIJVINGEN

Als laatste stap legt het Forum Standaardisatie de omschrijvingen voor aan het Nationale Beraad Digitale Overheid voor officiële vaststelling.

4.5 Planning

De onderstaande tabellen tonen de mogelijke planning van de vervolgactiviteiten:

DIGITOE GANKELIJK (EN 301 549 MET WCAG 2.0):

Activiteit	Planning
Vaststellen nieuwe omschrijving in Forum	14 juni 2017

DKIM, DMARC, DNSSEC, HTTPS EN HSTS, SPF EN TLS:

Activiteit	Planning
Uitvoeren openbare consultatie	1 augustus 2017 - 13 september 2017

Activiteit	Planning
Goedkeuren nieuwe omschrijvingen in Forum	11 oktober 2017
Vaststellen nieuwe omschrijvingen in NB	21 november 2017

DIGIKOPPELING:

Activiteit	Planning
Uitvoeren openbare consultatie	1 augustus 2017 - 13 september 2017
Goedkeuren nieuwe omschrijvingen in Forum	11 oktober 2017
Vaststellen nieuwe omschrijvingen in NB	21 november 2017

RESTERENDE STANDAARDEN:

Activiteit	Planning
Analyseren specifieke verplichtingen	1 juni 2017 - 30 juni 2017
Opstellen nieuwe omschrijvingen	1 juli 2017- 31 juli 2017
Uitvoeren openbare consultatie	1 augustus 2017 - 13 september 2017
Goedkeuren nieuwe omschrijvingen in Forum	11 oktober 2017
Vaststellen nieuwe omschrijvingen in NB	21 november 2017

4.6 Conclusies en aanbevelingen

Er zijn meerder scenario's mogelijk voor vaststelling van de nieuwe omschrijvingen, afhankelijk van het verschil met de huidige omschrijvingen. Als dit verschil klein is, dan kan vaststelling door het Forum Standaardisatie volstaan. Is het verschil groot, dan zullen al gauw een openbare consultatie en vaststelling door het Nationaal Beraad nodig zijn.

De verschillen tussen de nieuwe omschrijvingen en de huidige omschrijvingen zijn onderzocht. Op basis hiervan wordt geadviseerd om:

- de nieuwe omschrijving van DigiToegankelijk (EN 301 549 met WCAG 2.0) door het Forum Standaardisatie vast te laten stellen, zonder extra expertbijeenkomst en openbare consultatie.
- de nieuwe omschrijvingen van DKIM, DMARC, DNSSEC, HTTPS en HSTS, SPF en TLS als één pakket ter consultatie voor te leggen en, na goedkeuring door het Forum Standaardisatie, vast te laten stellen door het Nationaal Beraad;
- de nieuwe omschrijving van Digikoppeling 2.0 voor te leggen aan de deelnemers aan de consultatie van Digikoppeling 3.0 en de omschrijving, na goedkeuring door het Forum Standaardisatie, vast te laten stellen door het Nationaal Beraad.

De functioneel toepassingsgebieden van de overige standaarden zijn ook niet allemaal even duidelijk omschreven. Geadviseerd wordt om de minst duidelijk omschreven functioneel toepassingsgebieden opnieuw te omschrijven. Dit zijn de functioneel toepassingsgebieden van:

- NEN-ISO/IEC 27001
- NEN-ISO/IEC 27002
- STARTTLS en DANE
- WPA2 Enterprise
- Oauth en OpenID Connect
- SAML
- Aquo-standaard

Vaststelling van de nieuwe omschrijvingen en vervolgonderzoek naar de resterende standaarden kunnen parallel worden uitgevoerd aan de toetsingsprocedure voor de vergadering van het Nationaal Beraad van november 2017.

Definitief

Verduidelijking functioneel toepassingsgebieden

Eindrapport

VERDONCK
KLOOSTER&
ASSOCIATES

FS-20170419.02D

BIJLAGEN

A Voorbeelden van kenmerkende elementen

In het onderstaande worden de elementen waaruit de huidige omschrijvingen van de functioneel toepassingsgebieden zijn opgebouwd van een voorbeeld voorzien. De gebruikte voorbeelden kunnen meer dan één element bevatten. Om duidelijk te maken welk deel van de omschrijving wordt bedoeld, is dit deel steeds onderstreept.

A1. Functionaliteit ICT-dienst of -product

Met 'Functionaliteit ICT-dienst of -product' wordt bedoeld de functionaliteit waarmee een ICT-dienst of -product voorziet in een bepaalde gebruiksbehoefte.

Een voorbeelden van dit element kan worden gevonden in de omschrijving van het functioneel toepassingsgebied van SMeF 2.0:

De verzending van elektronische facturen door organisaties die deelnemen aan het economisch verkeer in Nederland (waaronder overheden) en de ontvangst hiervan door overheden.

Door deze omschrijving zijn overheidsorganisaties bij de aanschaf van een ICT-dienst of -product voor de verzending of de ontvangst van elektronische facturen verplicht om te kiezen voor een ICT-dienst of -product dat gebruik maakt van SMeF 2.0.

A2. Soort ICT-dienst of -product

Met 'Soort ICT-dienst of -product' wordt bedoeld een benoemde groep ICT-diensten of -producten die gemeenschappelijke kenmerken hebben (lees: voorzien in een vergelijkbare gebruiksbehoefte door een vergelijkbare functionaliteit te bieden).

Voorbeelden van dit element kunnen worden gevonden in de omschrijving van het functioneel toepassingsgebied van CMIS:

Het toegankelijk maken van ongestructureerde gegevens in content repositories van Content Management Systemen (CMS'en) en Document Management Systemen (DMS'en) met als doel deze gegevens uit te wisselen met andere CMS en DMS systemen.

Door deze omschrijving zijn overheidsorganisaties bij de aanschaf van een ICT-dienst of -product voor het toegankelijk maken van ongestructureerde gegevens in content repositories van CMS'en en DMS'en met als doel deze gegevens uit te wisselen met andere CMS'en en DMS'en verplicht om te kiezen voor een ICT-dienst of -product dat gebruik maakt van CMIS.

De verplichting geldt – in dit geval bewust – niet wanneer overheidsorganisaties een ICT-dienst of product willen aanschaffen voor het toegankelijk maken van ongestructureerde gegevens in content repositories van andere systemen dan CMS'en en DMS'en of met als doel deze gegevens uit te wisselen met andere systemen dan CMS'en en DMS'en.

A3. Gebruiksdoel ICT-dienst of -product

Met 'Gebruiksdoel ICT-dienst of -product' wordt bedoeld het doel waartoe gebruik wordt gemaakt van (de functionaliteit van) een ICT-dienst of -product.

Een voorbeeld van dit element kan worden gevonden in de omschrijving van het functioneel toepassingsgebied van BWB:

Elektronische verwijzing naar (delen van) geconsolideerde wetten en regelingen met het doel om deze met anderen te delen.

Door deze omschrijving zijn overheidsorganisaties bij de aanschaf van een ICT-dienst of -product voor elektronische verwijzing naar (delen van) geconsolideerde wetten en regelingen met het doel om deze met anderen te delen verplicht om te kiezen voor een ICT-dienst of -product dat gebruik maakt van BWB.

De verplichting zou niet gelden wanneer overheidsorganisaties een ICT-dienst of -product willen aanschaffen voor elektronische verwijzing naar (delen van) geconsolideerde wetten en regelingen zonder het doel om deze met anderen te delen.

A4. Gebruikskader ICT-dienst of -product

Met 'Gebruikskader ICT-dienst of -product' wordt bedoeld de context waarbinnen gebruik wordt gemaakt van (de functionaliteit van) een ICT-dienst of -product.

Voorbeelden van dit element kunnen worden gevonden in de omschrijving van het functioneel toepassingsgebied van VISI:

Formele communicatie tussen partijen in de bouwsector, zowel grond- weg en waterbouw, de burger & utiliteitsbouw als de installatiebranche.

Door deze omschrijving zijn overheidsorganisaties verplicht om bij de aanschaf van een ICT-dienst of -product voor formele communicatie tussen partijen in de grond-, weg- en waterbouw, de burger- en utiliteitsbouw en de installatiebranche te kiezen voor een ICT-dienst of -product dat gebruik maakt van VISI. De verplichting zou niet gelden wanneer overheidsorganisaties een ICT-

dienst of -product willen aanschaffen voor formele communicatie tussen partijen in andere deelsectoren.

A5. Gebruikers ICT-dienst of -product

Met 'Gebruikers ICT-dienst of -product' wordt bedoeld de organisaties of individuele eindgebruikers waardoor gebruik wordt gemaakt van (de functionaliteit van) een ICT-dienst of -product.

Voorbeelden van dit element kunnen worden gevonden in de omschrijving van het functioneel toepassingsgebied van SIKB0102:

Voor de digitale uitwisseling van archeologische informatie tussen opgravende instanties, vondstendepots en/of archeologische registers.

Door deze omschrijving zijn overheidsorganisaties verplicht om te kiezen voor een ICT-dienst of -product dat gebruik maakt van SIKB0102 bij de aanschaf van een ICT-dienst of product voor de digitale uitwisseling van archeologische informatie met opgravende instanties, vondstendepots of archeologische registers.

De verplichting zou niet gelden wanneer overheidsorganisaties een ICT-dienst of -product willen aanschaffen voor de digitale uitwisseling van archeologische informatie met andere organisaties dan opgravende instanties, vondstendepots of archeologische registers.

A6. Werking standaard

Met 'Werking standaard' wordt bedoeld de functionele of technische werking van de standaard.

Een voorbeeld van dit element kan worden gevonden in de omschrijving van het functioneel toepassingsgebied van TLS:

Het met behulp van certificaten beveiligen van de verbinding (op de transportlaag) tussen client- en serversystemen of tussen serversystemen onderling, voor zover deze gerealiseerd wordt met internettechnologie.

Door deze omschrijving zijn overheidsorganisaties verplicht om te kiezen voor een ICT-dienst of -product dat gebruik maakt van TLS bij de aanschaf van een ICT-dienst of -product voor het met certificaten beveiligen van verbindingen op internet.

De verplichting zou niet gelden wanneer overheidsorganisaties een ICT-dienst of -product willen aanschaffen voor de beveiliging van verbindingen op internet zonder gebruik te maken van certificaten.

A7. Naam standaard

Met 'Naam standaard' wordt bedoeld de volledige of verkorte naam van de standaard waarbij het functioneel toepassingsgebied is vermeld.

Een voorbeeld van dit element kan worden gevonden in de omschrijving van het functioneel toepassingsgebied van Digikoppeling 2.0:

Geautomatiseerde gegevensuitwisseling tussen informatiesystemen voor sectoroverstijgend berichtenverkeer, op basis van drie koppelvlakstandaarden:

- DK ebMS standaard voor meldingen tussen informatiesystemen
- DK WUS standaard voor de bevraging van informatiesystemen
- DK GB standaard voor de uitwisseling van grote berichten

Door deze omschrijving zijn overheidsorganisaties verplicht om te kiezen voor een ICT-dienst of -product dat gebruik maakt van Digikoppeling 2.0 bij de aanschaf van een ICT-dienst of -product voor geautomatiseerde gegevensuitwisseling tussen informatiesystemen voor sectoroverstijgend berichtenverkeer, op basis van de koppelvlakstandaarden DK ebMS, DK WUS en DK GB. DK staat voor Digikoppeling.

De verplichting zou niet gelden wanneer overheidsorganisaties een ICT-dienst of -product willen aanschaffen voor geautomatiseerde gegevensuitwisseling tussen informatiesystemen voor sectoroverstijgend berichtenverkeer op basis van andere koppelvlakstandaarden dan DK ebMS, DK WUS en DK GB.

A8. Nut standaard

Met 'Nut standaard' wordt bedoeld het voordeel dat toepassing van de standaard biedt ten opzichte van toepassing van geen of andere standaarden.

Een voorbeeld van dit element kan worden gevonden in de omschrijving van het functioneel toepassingsgebied van de Aquo-standaard:

Uitwisselen van uniforme gegevens over water tussen partijen die betrokken zijn bij het waterbeheer voor de kwaliteitsverbetering van het waterbeheer.

Door deze omschrijving zijn overheidsorganisaties verplicht om te kiezen voor een ICT-dienst of product dat gebruik maakt van de Aquo-standaard bij de aanschaf van een ICT-dienst of product voor het uitwisselen van uniforme gegevens over water met partijen die betrokken zijn bij het waterbeheer voor de kwaliteitsverbetering van het waterbeheer.

De verplichting zou niet gelden wanneer overheidsorganisaties een ICT-dienst of product willen aanschaffen voor het uitwisselen van uniforme gegevens over water met partijen die betrokken zijn bij het waterbeheer als dit niet bijdraagt aan de kwaliteitsverbetering van het waterbeheer.

Het is niet nodig om het nut van een standaard te vermelden in de omschrijving van het functioneel toepassingsgebied. De 'pas toe of leg uit'-lijst voorziet hiertoe bij elke standaard in een uitleg, waarin al op het nut van de standaard wordt ingegaan. Anders dan de omschrijving van het functioneel toepassingsgebied kan de uitleg worden gewijzigd zonder voorafgaande procedure. Het heeft daarom de voorkeur om het nut van de standaard in de uitleg op te nemen en niet in de omschrijving van het functioneel toepassingsgebied.

A9. Uitzondering/uitsluiting

Met 'Uitzondering/uitsluiting' wordt bedoeld de situatie of situaties waarin gebruik van de standaard – in uitzondering op de regel – niet verplicht is. De uitzondering of uitsluiting kan zowel een ICT-dienst of -product betreffen als een standaard.

Een voorbeeld van dit element kan worden gevonden in de omschrijving van het functioneel toepassingsgebied van WPA2 Enterprise:

Veilige, met behulp van een account geauthenticeerde toegang tot een wifi-netwerk van een (semi-) overheidsorganisatie.
Toegang tot publieke wifi-netwerken van overheden voor gasten zonder account is uitgesloten van de verplichting.

Door deze omschrijving hoeven overheidsorganisaties bij de aanschaf van een ICT-dienst of -product voor toegang tot een publiek wifi-netwerk voor gasten zonder account niet te kiezen voor een ICT-dienst of -product dat gebruik maakt van WPA2 Enterprise.

B Scores voor duidelijkheid

Op basis van de elementen waaruit de omschrijvingen zijn opgebouwd en de adviezen die hierover zijn uitgebracht, is een rekenmodel gemaakt waarmee op een schaal van 1 tot en met 5 uitspraken kunnen worden gedaan over de duidelijkheid van de omschrijvingen. Hierbij zij opgemerkt dat het rekenmodel alleen rekening houdt met de aan- of afwezigheid van de onderscheiden elementen. Het houdt geen rekening met de duidelijkheid waarmee de individuele elementen zijn omschreven.

De onderstaande tabel toont de berekende scores voor de duidelijkheid van de omschrijvingen:

Standaard	ICT-dienst of product					Standaard			Uitzondering/uitsluiting	Score	Domein
	Functionaliteit	Soort	Gebruiksdoel	Gebruikskader	Gebruikers	Werking	Naam	Nut			
Ades Baseline Profiles	X									4	Document & (Web)Content
Aquo-standaard	X				X	X		X		3	Water/Bodem
BWB	X		X							5	Juridische verwijzingen
CMIS	X	X				X				4	Document & (Web)Content
Digikoppeling 2.0	X						X			3	Stelselstandaarden
Digikoppeling 3.0	X			X					X	5	Stelselstandaarden
DigiToegankelijk (EN 301 549 met WCAG 2.0)	X									4	Document & (Web)Content
DKIM				X		X				1	Internet & Beveiliging
DMARC	X		X			X				4	Internet & Beveiliging
DNSSEC						X			X	1	Internet & Beveiliging

Standaard	ICT-dienst of product					Standaard			Uitzondering/uitsluiting	Score	Domein
	Functionaliteit	Soort	Gebruiksdoel	Gebruikskader	Gebruikers	Werking	Naam	Nut			
ECLI	X		X							5	Juridische verwijzingen
EML_NL	X			X						5	Overig
E-Portfolio NL	X				X					5	Onderwijs en Loopbaan
GEO-standaarden	X			X						5	Stelselstandaarden
HTTPS en HSTS	X	X								5	Internet & Beveiliging
IFC	X									4	Bouw
IPv6 en IPv4	X									4	Internet & Beveiliging
JCDR	X		X			X				4	Juridische verwijzingen
NEN-ISO/IEC 27001				X		X				1	Internet & Beveiliging
NEN-ISO/IEC 27002						X				1	Internet & Beveiliging
NL LOM	X									4	Onderwijs en Loopbaan
OAI-PMH	X		X						X	5	Onderwijs en Loopbaan
Oauth en OpenID Connect	X					X				3	Internet & Beveiliging
ODF	X									4	Document & (Web)Content
OWMS	X									4	Document & (Web)Content
PDF 1.7	X			X						5	Document & (Web)Content
PDF A1	X			X						5	Document & (Web)Content

Standaard	ICT-dienst of product					Standaard			Uitzondering/uitsluiting	Score	Domein
	Functionaliteit	Soort	Gebruiksdoel	Gebruikskader	Gebruikers	Werking	Naam	Nut			
PDF A2	X			X						5	Document & (Web)Content
SAML	X					X				3	Internet & Beveiliging
SETU	X									4	E-facturatie en Administratie
SIKB0101	X									4	Water/Bodem
SIKB0102	X				X					5	Water/Bodem
SKOS	X		X			X				4	Document & (Web)Content
SMeF 2.0	X				X					5	E-facturatie en Administratie
SPF						X				1	Internet & Beveiliging
STARTTLS en DANE			X	X		X				1	Internet & Beveiliging
Stosag	X									4	Overig
StUF	X									4	Stelselstandaarden
TLS		X				X				1	Internet & Beveiliging
VISI	X				X					5	Bouw
WDO Datamodel	X				X					5	E-facturatie en Administratie
WPA2 Enterprise		X				X			X	1	Internet & Beveiliging
XBRL en Dimensions	X									4	E-facturatie en Administratie

C Toets ideaaltypische syntactische structuur

Hieronder wordt de ideaaltypische syntactische structuur toegepast op de huidige omschrijvingen van de functioneel toepassingsgebieden van de volgende standaarden:

- BWB
- Digikoppeling 2.0
- DigiToegankelijk (EN 301 549 met WCAG 2.0)
- DNSSEC
- HTTPS en HSTS
- SETU
- TLS
- StUF

Deze selectie van standaarden is bepaald in overleg met het Bureau Form Standaardisatie. De selectie bevat zowel standaarden waarvan het functioneel toepassingsgebied duidelijk is omschreven als standaarden waarvan het functioneel toepassingsgebied duidelijker omschreven kan worden.

Voor iedere standaard wordt aangegeven welke delen van de huidige omschrijving volgens de ideaaltypische syntactische structuur behouden kunnen blijven en welke delen kunnen komen te vervallen.

C1. BWB

Het functioneel toepassingsgebied van BWB is momenteel als volgt omschreven:

Elektronische verwijzing naar (delen van) geconsolideerde wetten en regelingen met het doel om deze met anderen te delen.

Als we de ideaaltypische structuur toepassen op deze omschrijving, geeft dit het volgende resultaat:

Element	Invulling
Functionaliteit	Elektronische verwijzing naar (delen van) geconsolideerde wetten en regelingen
Gebruikers	Ontbreekt in de huidige omschrijving
Soort	Ontbreekt in de huidige omschrijving
Gebruikskader	Ontbreekt in de huidige omschrijving
Gebruiksdoel	met het doel om deze met anderen te delen.
Uitzondering/uitsluiting	Ontbreekt in de huidige omschrijving

Conclusie

De huidige omschrijving van het functioneel toepassingsgebied van BWB is duidelijk. Volgens de ideaaltypische structuur kan deze omschrijving geheel en onveranderd behouden blijven. De ideaaltypische structuur is dus geschikt voor deze standaard.

C2. Digikoppeling 2.0

Het functioneel toepassingsgebied van Digikoppeling 2.0 is momenteel als volgt omschreven:
Geautomatiseerde gegevensuitwisseling tussen informatiesystemen voor sectoroverstijgend berichtenverkeer, op basis van drie koppelvlakstandaarden:

- *DK ebMS standaard voor meldingen tussen informatiesystemen*
- *DK WUS standaard voor de bevraging van informatiesystemen*
- *DK GB standaard voor de uitwisseling van grote berichten*

Als we de ideaaltypische structuur toepassen op deze omschrijving, geeft dit het volgende resultaat:

Element	Invulling
Functionaliteit	Geautomatiseerde gegevensuitwisseling
Gebruikers	Ontbreekt in de huidige omschrijving
Soort	tussen informatiesystemen voor sectoroverstijgend berichtenverkeer.
Gebruikskader	Ontbreekt in de huidige omschrijving
Gebruiksdoel	Ontbreekt in de huidige omschrijving
Uitzondering/uitsluiting	Ontbreekt in de huidige omschrijving

Conclusie

Vanwege het advies om de volledige of verkorte naam van de standaard waarbij het functioneel toepassingsgebied is vermeld, niet toe te staan, komt het deel met de koppelvlakstandaarden DK ebMS, DK WUS en DK GB (DK staat voor Digikoppeling) te vervallen. Wat overblijft is een (te) ruim toepassingsgebied, dat nader kan worden gepreciseerd met behulp van elementen van de ideaaltypische structuur.

Het functioneel toepassingsgebied van Digikoppeling 3.0, die is aangemeld en in procedure genomen voor opname op de 'pas toe of leg uit'-lijst (maar zal worden teruggetrokken), bevat de nodige aanknopingspunten voor een nieuwe, duidelijkere omschrijving:

Element	Invulling
Functionaliteit	Alle digitale gegevensuitwisseling met behulp van gestructureerde berichten
Gebruikers	Ontbreekt in de huidige omschrijving

Element	Invulling
Soort	die plaatsvindt met voorzieningen die onderdeel zijn van de GDI, waaronder de basisregistraties,
Gebruikskader	of die sectoroverstijgend is.
Gebruiksdoel	Ontbreekt in de huidige omschrijving
Uitzondering/uitsluiting	Uitgezonderd is de verplichting tot het gebruik van NEN3610 (geo-standaarden) en uitgezonderd zijn de gevallen waarin de aanbieder van gegevens vaststelt dat geen noodzaak bestaat om de afnemer van de gegevens te authenticeren.

De concept-omschrijving van het functioneel toepassingsgebied van Digikoppeling 3.0 is duidelijk. Volgens de ideaaltypische structuur kan deze omschrijving geheel en onveranderd behouden blijven. De ideaaltypische structuur is dus geschikt voor deze standaard.

C3. DigiToegankelijk (EN 301 549 met WCAG 2.0)

Het functioneel toepassingsgebied van DigiToegankelijk (EN 301 549 met WCAG 2.0) is momenteel als volgt omschreven:

EN 301 549 is van toepassing op webgebaseerde informatie-, interactie-, transactie- en participatiediensten.

Als we de ideaaltypische structuur toepassen op deze omschrijving, geeft dit het volgende resultaat:

Element	Invulling
Functionaliteit	Webgebaseerde informatie-, interactie-, transactie- en participatiediensten.
Gebruikers	Ontbreekt in de huidige omschrijving
Soort	Ontbreekt in de huidige omschrijving
Gebruikskader	Ontbreekt in de huidige omschrijving
Gebruiksdoel	Ontbreekt in de huidige omschrijving
Uitzondering/uitsluiting	Ontbreekt in de huidige omschrijving

Conclusie

De huidige omschrijving is duidelijk en kan volgens de ideaaltypische structuur behouden blijven, zij het zonder het deel 'EN 301 549 is van toepassing op'. Het functioneel toepassingsgebied kan eventueel nader worden gepreciseerd door in de omschrijving op te nemen dat in dit geval websites en webapplicaties worden bedoeld ('Soort ICT-dienst of -product'). De ideaaltypische structuur is dus geschikt voor deze standaard.

C4. DNSSEC

Het functioneel toepassingsgebied van DNSSEC is momenteel als volgt omschreven:

Het registreren en in DNS publiceren van internet-domeinnamen ('signing'). De registratieverplichting geldt enkel indien 'signed domain names' bij een registerhouder van een top-level domein (zoals SIDN voor .NL) geautomatiseerd aangevraagd kunnen worden; Het vertalen van domeinnamen naar internetadressen en vice versa ('validation enabled resolving'). Validatie is niet verplicht voor systemen die niet direct aan het publieke internet gekoppeld zijn (bijvoorbeeld clients/werkplekken binnen een LAN en interne DNS-systemen).

Als we de ideaaltypische structuur toepassen op deze omschrijving, geeft dit het volgende resultaat:

Element	Invulling
Functionaliteit	Ontbreekt in de huidige omschrijving
Gebruikers	Ontbreekt in de huidige omschrijving
Soort	Domeinnamen
Gebruikskader	Ontbreekt in de huidige omschrijving
Gebruiksdoel	Ontbreekt in de huidige omschrijving
Uitzondering/uitsluiting	met uitzondering van systemen die niet direct aan het publieke internet gekoppeld zijn (bijvoorbeeld clients/werkplekken binnen een LAN en interne DNS-systemen).

Conclusie

Vanwege het advies om de functionele of technische werking van de standaard niet toe te staan, komt een groot deel van de omschrijving te vervallen. De uitzondering is behouden, omdat dit de situatie of situaties verduidelijkt waarin gebruik van de standaard – in uitzondering op de regel – niet verplicht is. Dit zou ook verduidelijkt kunnen worden door aan te geven dat het gaat om domeinnamen waarmee met burgers of bedrijven ('Gebruikers ICT-dienst of -product') wordt gecommuniceerd ('Functionaliteit ICT-dienst of -product'). De ideaaltypische structuur is dus geschikt voor deze standaard.

C5. HTTPS en HSTS

Op dit moment ligt het expertadvies voor HTTPS en HSTS ter consultatie. Het functioneel toepassingsgebied is als volgt voorgesteld:

Het beveiligen van de communicatie tussen clients (zoals webbrowsers) en servers voor alle via internet benaderbare websites en -webservices.

Als we de ideaaltypische structuur toepassen op deze omschrijving, geeft dit het volgende resultaat:

Element	Invulling
Functionaliteit	De communicatie
Gebruikers	Ontbreekt in de huidige omschrijving
Soort	tussen clients (zoals webbrowsers) en servers voor alle via internet benaderbare websites en -webservices.
Gebruikskader	Ontbreekt in de huidige omschrijving
Gebruiksdoel	Ontbreekt in de huidige omschrijving
Uitzondering/uitsluiting	Ontbreekt in de huidige omschrijving

Conclusie

Vanwege het advies om de functionele of technische werking van de standaard niet toe te staan, komt 'Het beveiligen van' te vervallen. Wat overblijft is duidelijk genoeg om te kunnen concluderen dat de ideaaltypische structuur geschikt is voor deze standaard.

C6. SETU

Het functioneel toepassingsgebied van SETU is momenteel als volgt omschreven:

De elektronische berichtenuitwisseling rondom de bemiddeling/inhuur van flexibele arbeidskrachten.

Als we de ideaaltypische structuur toepassen op deze omschrijving, geeft dit het volgende resultaat:

Element	Invulling
Functionaliteit	De elektronische berichtenuitwisseling
Gebruikers	Ontbreekt in de huidige omschrijving
Soort	Ontbreekt in de huidige omschrijving
Gebruikskader	rondom de bemiddeling/inhuur van flexibele arbeidskrachten.
Gebruiksdoel	Ontbreekt in de huidige omschrijving
Uitzondering/uitsluiting	Ontbreekt in de huidige omschrijving

Conclusie

De huidige omschrijving is duidelijk en kan volgens de ideaaltypische structuur geheel en onveranderd behouden blijven. De ideaaltypische structuur is dus geschikt voor deze standaard.

C7. StUF

Het functioneel toepassingsgebied van StUF is momenteel als volgt omschreven:

Uitwisseling en bevraging van basisgegevens die behoren tot een aantal wettelijk vastgestelde basisregistraties, zoals Personen (GBA), Adressen (BRA), Gebouwen (BGA), Kadaster (BRK), Nieuw Handelsregister (NHR) en Waarde Onroerende Zaken (WOZ); uitwisseling en bevraging van zaakgegevens die behoren tot de producten- en dienstenportfolio van gemeenten; uitwisseling van domein- of sectorspecifieke gegevens waarin ook basis- en/of zaakgegevens voorkomen en waarvoor geen andere (inter)nationale (XML-gebaseerde) berichtenstandaard is vastgesteld.

Als we de ideaaltypische structuur toepassen op deze omschrijving, geeft dit het volgende resultaat:

Element	Invulling
Functionaliteit	Uitwisseling en bevraging van basisgegevens die behoren tot een aantal wettelijk vastgestelde basisregistraties, zoals Personen (GBA), Adressen (BRA), Gebouwen (BGA), Kadaster (BRK), Nieuw Handelsregister (NHR) en Waarde Onroerende Zaken (WOZ); uitwisseling en bevraging van zaakgegevens die behoren tot de producten- en dienstenportfolio van gemeenten; uitwisseling van domein- of sectorspecifieke gegevens waarin ook basis- en/of zaakgegevens voorkomen
Gebruikers	Ontbreekt in de huidige omschrijving
Soort	Ontbreekt in de huidige omschrijving
Gebruikskader	Ontbreekt in de huidige omschrijving
Gebruiksdoel	Ontbreekt in de huidige omschrijving
Uitzondering/uitsluiting	en waarvoor geen andere (inter)nationale (XML-gebaseerde) berichtenstandaard is vastgesteld.

Conclusie

De huidige omschrijving kan volgens de ideaaltypische structuur geheel en onveranderd behouden blijven. De ideaaltypische structuur is dus geschikt voor deze standaard. Hierbij zij opgemerkt dat de huidige omschrijving vrij complex is en daardoor niet voor iedereen meteen duidelijk zal zijn.

C8. TLS

Het functioneel toepassingsgebied van TLS is momenteel als volgt omschreven:

Het met behulp van certificaten beveiligen van de verbinding (op de transportlaag) tussen client- en serversystemen of tussen serversystemen onderling, voor zover deze gerealiseerd wordt met internettechnologie.

Als we de concept-structuur toepassen op deze omschrijving, geeft dit het volgende resultaat:

Element	Invulling
Functionaliteit	Ontbreekt in de huidige omschrijving
Gebruikers	Ontbreekt in de huidige omschrijving
Soort	De verbinding tussen client- en serversystemen of tussen serversystemen onderling, voor zover deze gerealiseerd wordt met internettechnologie.
Gebruikskader	Ontbreekt in de huidige omschrijving
Gebruiksdoel	Ontbreekt in de huidige omschrijving
Uitzondering/uitsluiting	Ontbreekt in de huidige omschrijving

Conclusie

Vanwege het advies om de functionele of technische werking van de standaard niet toe te staan, komt de tekst over de certificaten en transportlaag te vervallen. Het deel met internettechnologie is behouden, omdat dit verduidelijkt om wat voor soort ICT-dienst of -product het gaat (internetverbindingen). Het functioneel toepassingsgebied kan nader worden gepreciseerd door in de omschrijving op te nemen waarvoor de internetverbindingen worden gebruikt, namelijk de uitwisseling van gegevens ('Functionaliteit ICT-dienst of -product'). De ideaaltypische structuur is dus geschikt voor deze standaard. Zie ook de paragraaf over HTTPS en HSTS.