2A Wet digitale overheid en open standaarden

Vergadering:	Forum Standaardisatie 12 april 2023
Agendapunt:	2A
Documentnummer:	FS-20230412.2A
Aan:	Forum Standaardisatie
Van:	Bureau Forum Standaardisatie
Opsteller:	Ludwig Oberendorff
Meelezer:	
Datum:	28 maart 2023
Versie:	
Bijlagen:	Geen (links naar Wetsvoorstel en Memorie van Toelichting in deze notitie)
Rechten:	CC0 publieke domein verklaring

Ter bespreking

a. Inleiding

De Eerste Kamer heeft dinsdag 21 maart ingestemd met het wetsvoorstel Digitale overheid (Wdo). Die wet is van groot belang voor het werk van het Forum Standaardisatie, en het Forum heeft ook bijgedragen aan de totstandkoming ervan, en er formeel op gereageerd in eerdere internetconsultaties. Het Forum en zijn werkzaamheden komen uitgebreid aan de orde in de Memorie van Toelichting (MvT).

Artikel 3 van de wet regelt de mogelijkheid om open standaarden aan 'overheidsorganisaties' te verplichten (via een Algemene Maatregel van Bestuur: AMvB). Dit artikel 3 treedt een dag na de publicatie van de wet in het Staatsblad in werking.

Twee standaarden staan klaar om via deze grondslag te worden verplicht. Het gaat om de digitoegankelijkheid standaard WCAG (op dit moment al verplicht 'met als grondslag een AMvB via de Grondwet'), en om de anti-website-phishing standaarden HTTPS en HSTS (het slotje op de website). De concept Algemene Maatregel van Bestuur over HTTPS en HSTS is eerder geconsulteerd, de Raad van State heeft erover geadviseerd, en er is over besloten in de Ministerraad. Vorige Forumvergadering stond een FAQ over de komende wettelijk verplichting van deze standaarden ter kennisname op de agenda.

Link naar Wetsvoorstel Digitale Overheid

Link naar Memorie van Toelichting

Link naar FAQ over verplichting HTTPS en HSTS voor overheidswebsites

b. Een paar Wdo-hoofdpunten ten aanzien van open standaarden

1) Een open standaard kan worden aangewezen (*i.e. verplicht*), indien dit noodzakelijk en proportioneel is voor:
   a) de werking;
   b) de veiligheid;
   c) de betrouwbaarheid;
   d) de duurzame toegankelijkheid; of

e) de doelmatigheid van het elektronische verkeer met of tussen bestuursorganen (*dus ook met burgers en bedrijven*); of
f) indien dit voortvloeit uit internationale verplichtingen.

2) Het organisatorisch werkingsgebied van zo'n verplichting is ruim (MvT, p.59): 'overheidsorganisaties', in de zin van de a+b bestuursorganen, colleges (art.1:1 eerste en tweede lid Algemene wet bestuursrecht/Awb) en Rechtspersonen met een Wettelijke taak.
Per standaard/AMvB kan de verplichting desgewenst worden ingeperkt.

3) De standaard moet vrij van licentierechten kunnen worden gebruikt. De specificaties ervan moeten vrij, of eventueel tegen een redelijke vergoeding beschikbaar zijn.

4) De noodzaak van wetgeving wordt onderbouwd met het beperkte effect dat de 'pas toe of leg uit verplichting' en de nadere bestuurlijke afspraken daarover bleek te hebben. Ondermeer gezien de vrijblijvendheid er van, en het gebrek aan toezicht (Mvt, p.7).

5) 'Pas toe of leg uit' blijft waardevol, maar is voor sommige standaarden onvoldoende. Daar moeten overheidsorganisaties de standaard eenvoudigweg toepassen (Mvt, p.7).
Met wettelijke verplichting zal evenwel terughoudend worden omgegaan, en het ligt niet in de verwachting dat de lijst van open standaarden in zijn geheel en/of voor de gehele (semi) publieke sector verplichtend wordt (Mvt, p.60).

6) Als tot verplichting wordt overgegaan zal dat doorgaans gaan om een open standaard die al op de 'pas toe of leg uit'-lijst staat, maar dat hoeft niet. Voor nieuwe standaarden kan de procedure voor plaatsing op de lijst en verplichting op grond van deze wet parallel lopen (Mvt, p.60).
Wanneer een standaard wettelijk verplicht wordt, zal deze van de 'pas toe of leg uit' lijst worden verwijderd (Mvt, p.8).

7) Toezicht, monitoring en derdenwerking
   Qua verplichte open standaarden geldt het reguliere toezicht, en de reguliere ministeriële verantwoordelijkheid (wat dat voor de verschillende overheidsdomeinen betekent staat op p.32, 33 en 86).

   Het gebruik van een verplichte standaard zal jaarlijks worden gemonitord (Mvt, p.8)

   Bij een verplichting kunnen nadere regels worden gesteld, bijvoorbeeld dat er een actuele verklaring over de toepassing van de standaard door de overheidsorganisaties dient te worden gepubliceerd, of dat een auditplicht wordt opgelegd (Mvt, p.61).

   De toepassing van een verplichte standaard strekt tevens tot bescherming van burgers en bedrijven (Mvt, p.61). Dat betekent dat (ook belangengroepen) van burgers en bedrijven bezwaar kunnen aantekenen, wanneer de standaarden niet worden toegepast (bijvoorbeeld in een digitale overheidsdienst, of een aanbesteding).

8) In de Memorie van Toelichting wordt al uitgebreid ingegaan op het belang van open standaarden voor informatieveiligheid. Naast HTTPS en TLS, ook de anti-email-phishing standaarden DKIM, SPF en DNSSEC (Mvt, p.9, 41, 61). De Memorie onderstreept de noodzaak van toepassing door alle overheidsorganisaties, en rechtvaardigt de proportionaliteit van de (mogelijkheid tot) wettelijke verplichting, in grote mate door het belang juist bij deze standaarden achterblijvers over de streep te trekken.
   De urgentie die de Memorie ten aanzien daarvan uitademt kan, nu 5 jaar later, alleen maar zijn toegenomen, getuige de grote groep achterblijvers in de laatste iv-metingen.

Enkele nieuwsberichten:

Link naar Senaat steunt voorstellen digitale overheid - Eerste Kamer der Staten-Generaal

Link naar Wettelijke verplichting van standaarden vormt ‘een bezemwagen’ | Forum Standaardisatie

c. Bespreekpunten

- "De Minister van BZK zal het Forum Standaardisatie betrekken bij de voorbereiding van een algemene maatregel van bestuur(…)" (MvT, p.8)
  In de MvT wordt (naast Digitoegankelijk + HTTPS/HSTS) duidelijk voorgesorteerd op de anti-email-phishing standaarden (zoals DKIM, SPF en DNSSEC, zie ondermeer p.61).
  Wordt verplichting van die standaarden momenteel als eerstvolgende overwogen?

- "Het gebruik van een verplichte standaard zal jaarlijks worden gemonitord." (MvT, p.8).
  Daarvoor lijkt IV-meting Forum Standaardisatie in de rede te liggen.

- T.a.v. toezicht & eID is het nodige in de Kamers aan de orde geweest, *heeft dat ook invloed op de toezichtsconstructie t.a.v. open standaarden?*