Forum Standaardisatie
www.forumstandaardisatie.nl
forumstandaardisatie@logius.nl
Bureau Forum Standaardisatie
gehuisvest bij Logius
Postadres
Postbus 96810
2509 JE Den Haag
Bezoekadres
Wilhelmina van Pruisenweg 52
2595 AN Den Haag
Bij bezoek aan Logius is legitimatie verplicht

notitie

Opname HTTPS & HSTS als verplichte standaard op de lijst met open standaarden

FORUM STANDAARDISATIE

Agendapunt:	FS-20170419.02A
Betreft:	Opname HTTPS & HSTS als verplichte standaard op de lijst met open standaarden
Aan:	Forum Standaardisatie
Van:	Stuurgroep Standaardisatie
Datum:	6 april 2017

Aanleiding en achtergrond

Door het Forum Standaardisatie worden momenteel de standaarden HTTP (versie 1.1 en 2), HTTPS en HSTS aanbevolen. Dit terwijl de standaard TLS verplicht is conform 'pas toe of leg uit'. Gezien de raakvlakken tussen deze standaarden blijkt dat in de praktijk het verschil in status tussen deze standaarden verwarrend is voor organisaties. Ook is er een toenemende roep om HTTPS te verplichten voor alle overheidswebsites. Begin 2017 heeft, in antwoord op Kamervragen, minister Plasterk van het ministerie van BZK aangegeven om na de invoering van de Wet generieke digitale infrastructuur (wet GDI) HTTPS voor alle overheidswebsites te willen verplichten. Voor het wettelijk verplichten van standaarden via de wet GDI zal eventueel een aparte procedure worden gevolgd.

De HTTPS-standaard (Hypertext Transfer Protocol Secure) wordt gebruikt om webverkeer te beschermen tegen onbevoegde partijen die mee willen lezen (passieve aanvallers) of het webverkeer willen manipuleren (actieve aanvallers). HSTS is een beveiligingsmechanisme dat het gebruik van een veilige (HTTPS) verbinding afdwingt.

Geadviseerd wordt om HTTPS & HSTS te verplaatsen naar de 'pas toe of leg uit'-lijst. Gelet op het toepassingsgebied wordt ook geadviseerd om HTTP (versie 1.1 en 2) te verwijderen van de aanbevolen lijst en deze onderdeel te maken van de opname van HTTPS en HSTS.

Betrokkenen en proces

Jasmijn Wijn, procedurebegeleider open standaarden in opdracht van het Bureau Forum Standaardisatie, heeft het onderzoek uitgevoerd. Hiertoe heeft een intakegesprek plaatsgevonden met Bart Knubben, adviseur internet- en beveiligingsstandaarden van het Bureau Forum Standaardisatie. Het expertadvies is opgesteld op basis van de intake en een aantal gesprekken met (potentiële) gebruikers en andere kennishebbers. Tijdens de openbare consultatie van het expertadvies van 24 februari – 25 maart 2017 zijn vijf reacties ontvangen. Het waren overwegend aanvullingen op het expertadvies en positief over de verplichting van HTTPS en HSTS. De reacties zijn in overleg met de betrokken partijen verwerkt in dit forumadvies.

Consequenties en vervolgstappen

Er zijn geen specifieke risico's verbonden aan de keuze.

Het Forum Standaardisatie zal op basis van het Forumadvies en de relevante inzichten uit de openbare consultatie een advies aan het Nationaal Beraad opstellen. Het Nationaal Beraad bepaalt uiteindelijk op basis van het advies of de status van HTTPS en HSTS wordt gewijzigd van 'aanbevolen' naar 'verplicht'.

Gevraagd besluit

Het Forum Standaardisatie wordt gevraagd om in te stemmen met onderstaand advies:

Het Forum Standaardisatie adviseert het Nationaal Beraad Digitale Overheid om:
1. De status van HTTPS en HSTS te wijzigen van 'aanbevolen' naar 'verplicht'.
2. In te stemmen met de additionele adviezen ten aanzien van de adoptie van de standaard.

Ad 1 Toelichting wijziging status HTTPS en HSTS
De standaard HTTPS in combinatie met HSTS voldoet aan de criteria voor opname op de lijst met (conform 'pas toe of leg uit') verplichte standaarden. Het Forum Standaardisatie en het Nationaal Beraad wordt geadviseerd om HTTPS en HSTS inclusief de veilige configuratie conform NCSC[1] op te nemen op de 'pas toe of leg uit'-lijst voor onderstaand functioneel toepassingsgebied en organisatorisch werkingsgebied.

Als functioneel toepassingsgebied wordt geadviseerd:
Het beveiligen van de communicatie tussen clients (zoals webbrowsers) en servers voor alle via het internet benaderbare websites en webservices.

Als organisatorisch werkingsgebied wordt geadviseerd:
Nederlandse overheden (Rijk, provincies, gemeenten en waterschappen) en instellingen uit de (semi-) publieke sector.
Hiermee dienen HTTPS en HSTS te worden verwijderd van de lijst met aanbevolen standaarden. Gelet op het toepassingsgebied wordt ook geadviseerd om HTTP (versie 1.1 en 2) te verwijderen van de aanbevolen lijst en deze onderdeel te

[1] Zie ICT-beveiligingsrichtlijnen voor Webapplicaties uit 2015 (met name richtlijn U/WA.05 onder "05 Versleutel communicatie") en de ICT-beveiligingsrichtlijnen voor Transport Layer Security uit (TLS), november 2014.

maken van de opname van HTTPS en HSTS. Ook is het advies om TLS te behouden op de 'pas toe of leg uit'-lijst omdat deze standaard ook toegepast kan worden om andersoortige communicatie dan webverkeer te beveiligen.

Voor webservices is het functioneel toepassingsgebied alleen van toepassing bij 'server to client'-interactie, niet voor 'server to server'-interactie.

Ad 2 Additionele adviezen ten aanzien van de adoptie van de standaarden
Ten aanzien van de adoptie van de standaard worden de volgende oproepen gedaan:

1. Als adoptie-impuls af te spreken dat alle overheidswebsites HTTPS en HSTS inclusief de veilige configuratie conform NCSC uiterlijk eind 2018 hebben ingevoerd. Dit is een aanvulling op de bestaande adoptieimpuls van het Nationaal Beraad. Daarbij is afgesproken dat HTTPS voor eind 2017 moet zijn ingevoerd voor die overheidswebsites waar burgers en/of bedrijven gegevens invoeren (zoals in een contactformulier) of waarbij gegevens vooringevuld zijn.
2. Bij de opname op de 'pas toe of leg uit'-lijst de volgende oproepen te doen:
   - Aan NCSC om de ontwikkelingen rondom HTTPS en HSTS te volgen en de genoemde ICT-beveiligingsrichtlijnen te actualiseren wanneer hier aanleiding toe is. Daarnaast wordt het NCSC opgeroepen om de ICT-beveiligingsrichtlijnen ook in het Engels beschikbaar te maken.
   - Aan de minister van Binnenlandse Zaken en Koninkrijksrelaties om, na inwerkingtreding van de wet GDI, niet alleen HTTPS maar ook HSTS en de veilige configuratie conform NCSC in onderzoek te nemen voor verplichting via een algemene maatregel van bestuur (AMvB).
   - Aan overheden de aanbevelingen uit de NCSC-factsheet 'Veilig beheer van digitale certificaten' (2012) te volgen. Onderdeel van deze factsheet is ook de aanschaf van een extra set 'back up'-certificaten. Hierdoor kan de impact van een hack bij of faillissement van een CA, zoals bij DigiNotar, worden beperkt.
   - Aan Platform Internetstandaarden om meer toelichting en achtergrondinformatie te geven bij de test op Internet.nl. Hiervoor kan met onder andere KING/IBD samengewerkt worden. Zij krijgt regelmatig vragen van gemeenten over de testresultaten.
   - Aan het Forum Standaardisatie om de voortgang van de adoptie van HTTPS en HSTS inclusief de veilige configuratie conform NCSC te monitoren en hierover aan het Nationaal Beraad te rapporteren.
   - Overheden met websites met digitale dienstverlening, bijvoorbeeld door middel van DigiD, dienen te overwegen om hun domein op een pre-loading lijst te plaatsen om te voorkomen dat de landingspagina via HTTP benaderd kan worden.

De opgeroepen partijen worden gevraagd om één jaar na opname van de standaard over de voortgang op deze punten te rapporteren aan het Forum Standaardisatie.

Toelichting

1. Waar gaat het inhoudelijk over?

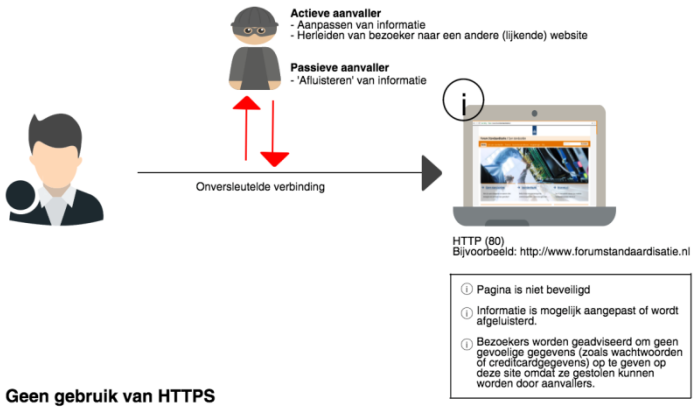
De overheid gebruikt in toenemende mate websites voor informatieverstrekking en dienstverlening. Met deze toenemende digitalisering is ook het beveiligingsrisico aanzienlijk toegenomen. Dit vraagt om aandacht voor de dreiging van digitale (economische) spionage en identiteitsdiefstal. Zonder adequate beveiligingsmaatregelen kan in een kort tijdsbestek een grote hoeveelheid aan informatie op de facto anonieme wijze worden verzameld. Informatie kan worden geblokkeerd, en onder bepaalde voorwaarden worden aangepast en vervalst.

De Nederlandse overheid heeft vanuit haar rol de taak en verplichting om (toevertrouwde) vertrouwelijke informatie te beschermen tegen afluisteren door aanvallers, zoals criminele partijen. Onder de te beschermen informatiestromen valt ook feitelijk communicatie tussen overheidspartijen, tussen de overheid en bedrijven en tussen overheden en burgers door middel van websites en webservices.

HTTPS

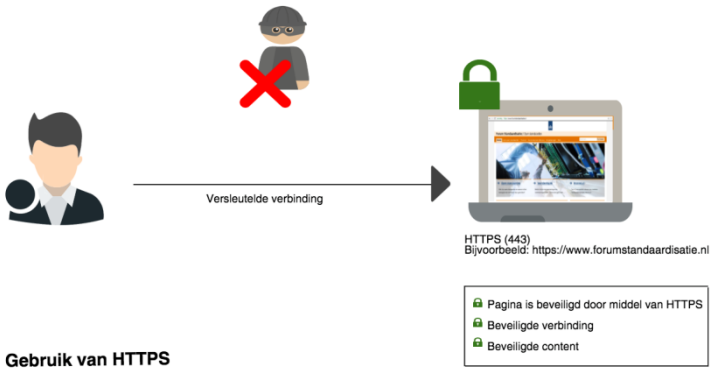
De HTTPS-standaard (Hypertext Transfer Protocol Secure) wordt gebruikt om webverkeer te beschermen tegen onbevoegde partijen die mee willen lezen (passieve aanvallers) of het webverkeer willen manipuleren (actieve aanvallers). De standaard legt vast hoe het HTTP-protocol beveiligd kan worden door gebruik te maken van TLS. HTTPS wordt ingezet voor het beveiligen van de communicatie tussen een client en een server op onderstaande aspecten:

Vertrouwelijkheid	Het versleutelen van verstuurde gegevens (encryptie)[2], zodat onbevoegde inzage niet mogelijk is.
Integriteit	Controle op de integriteit van de informatie zodat aanpassing van de uitgewisselde gegevens niet mogelijk is.
Authenticatie	Door de identiteit van de webserver te controleren kan zeker worden gesteld dat de website daadwerkelijk de juiste website is en bezoekers van een website niet zijn omgeleid naar een andere website.



Geen gebruik van HTTPS

[2] IP-adressen en domeinnamen worden niet versleuteld door HTTPS.



Figuur 1. Weergave functionaliteit van HTTPS voor websites.

Toepassing HTTPS in combinatie met HSTS
Eind 2016 is HSTS (RFC 6797) toegevoegd aan de lijst met aanbevolen standaarden onder HTTPS. Het advies is om HTTPS altijd te gebruiken in combinatie met HTSTS. Wanneer in dit advies gesproken wordt over de verplichting van HTTPS dan betreft dit HTTPS in combinatie met HSTS.

HSTS staat voor HTTP Strict Transport Security en is een beveiligingsmechanisme dat het gebruik van een veilige (HTTPS) verbinding afdwingt. Wanneer een bezoeker een onbeveiligde (HTTP) website wil bezoeken wordt deze, na het eerste bezoek, automatisch doorgestuurd naar een HTTPS-website. Indien dit niet mogelijk is krijgt de bezoeker een foutmelding. Als een website HSTS gebruikt, vereist een browser voor elke terugkerende bezoeker dat de website voor een vooraf bepaalde periode, opnieuw via HTTPS wordt aangeboden. Dit draagt bij aan de voorkoming van man-in-the-middle-aanvallen, omdat potentiële aanvallers het verkeer niet kunnen omleiden via HTTP. Deze termijn kan van minuten tot oneindig worden ingesteld.

HSTS is wel device- en browserafhankelijk. Dit wil zeggen dat het mechanisme alleen werkt wanneer een persoon bij herhaald bezoek hetzelfde device en dezelfde browser gebruikt. Het mechanisme werkt niet wanneer een persoon bij het eerste bezoek Safari en bij de tweede keer Google Chrome gebruikt. Of bij het eerste bezoek een laptop en bij het tweede bezoek een mobiele telefoon. HSTS biedt dus beveiliging ná het eerste bezoek vanaf de betreffende browser. Die beveiliging werkt zolang de persoon terugkeert binnen de gestelde HSTS-verlooptijd. Deze termijn kan van minuten tot oneindig worden ingesteld.

<u>HSTS preloading</u>
HSTS preloading is een mechanisme waarbij het gebruik van HTTPS ook bij het eerste bezoek wordt afgedwongen. Chrome, Firefox en Safari maken gebruik van een lijst met hosts die HSTS preloading toepassen. De browser (Chrome, Firefox of Safari) zal websites die op de lijst staan altijd met HTTPS benaderen. Wanneer een gebruiker HTTP:// invoert passen de bovengenoemde browsers automatisch HTTPS toe. Het gebruik van HSTS preloading vereist een goede implementatie van HTTPS. Indien dit niet het geval is zal er geen verbinding tot stand kunnen worden gebracht en is de website niet beschikbaar voor bezoekers. Er zijn goede implementatie voorbeelden en handreikingen beschikbaar, zoals die van het NCSC.

<u>2. Hoe is het proces verlopen?</u>
Om te komen tot dit Forumadvies zijn de volgende stappen doorlopen:

- Door de procedurebegeleider is een intakegesprek gevoerd met de indiener, Bart Knubben van het Bureau Forum Standaardisatie.
- Vervolgens is onderzoek in de vorm van deskresearch en interviews gedaan, waarbij HTTPS en HSTS opnieuw zijn getoetst aan de toetsingscriteria van het Forum Standaardisatie.
- Op basis van dit onderzoek is een eerste conceptadvies opgesteld.
- Vervolgens zijn zeven interviews gehouden met (potentieel) gebruikers en andere kennishebbers om de bevindingen de toetsen en waar nodig aan te vullen.
- Het advies is vervolgens ten behoeve van de publieke consultatieronde gepubliceerd.
- Uit de publieke consultatie zijn vijf reacties ontvangen, welke zijn verwerkt in dit Forumadvies.

3. Hoe scoort de standaard op de toetsingscriteria?

Toegevoegde waarde
De Nederlandse overheid moet vertrouwelijke informatie beschermen tegen afluisteren door aanvallers, zoals criminele partijen. Hieronder valt ook de communicatie tussen overheidspartijen, tussen overheden en bedrijven, en tussen overheden en burgers via websites of webservices. Het is ook belangrijk dat burgers en bedrijven bij het bezoeken van een overheidswebsite er zeker van kunnen zijn dat deze ook daadwerkelijk van de overheid is en dat informatie niet is aangepast of kan worden afgeluisterd/aangepast. Het kan hierbij gaan om gebruikersnamen, wachtwoorden en andere gevoelige informatie, maar ook om op het oog minder gevoelige gegevens zoals zoekgedrag op een website.

Overheidsorganisaties zijn op dit moment zelf verantwoordelijk om te bepalen of hun website gevoelige informatie bevat. Indien dit het geval is zijn zij verplicht om passende beveiligingsmaatregelen te nemen. Geadviseerd wordt om alle vormen van surfgedrag als privé en gevoelig te beschouwen en als zodanig te beveiligen. Hierdoor wordt voorkomen dat op basis van subjectiviteit beslissingen worden genomen over welke informatie gevoelig is en welke niet. Het verplichten van HTTPS en HSTS voor alle websites en webservices zorgt ervoor dat de webverkeer tussen overheden, burgers en bedrijven beveiligd is.

Implementatie van HTTPS
De kosten om HTTPS te implementeren en afname van de snelheid van de website worden vaak als argumenten tegen het gebruik van de standaard gebruikt. De kosten om de standaarden technisch te implementeren en te onderhouden zijn echter doorgaans beperkt, zeker als deze worden afgemeten tegen de totale exploitatiekosten van een website. De kosten van het aanschaffen en beheren van een HTTPS-certificaat is ongeveer €600,00 per organisatie. Door het versleutelen en ontsleutelen van gegevens en het uitwisselen van certificaten worden de servers extra belast. Hoewel deze aanvullende belasting niet groot is, is het wel aan te raden om dit voorafgaand aan de overgang naar HTTPS te toetsen.

Open standaardisatieproces
HTTPS en HSTS worden beheerd door de internationale beheerorganisatie Internet Engineering Task Force (IETF). Geconcludeerd wordt dat het van IETF voldoende open is: IETF kent goed gedocumenteerde en open beheerprocedures, er is geen lidmaatschap, het beheerproces en de besluitvorming hieromtrent is open en transparant. Documentatie is kosteloos verkrijgbaar.

Draagvlak
De Autoriteit Persoonsgegevens heeft op basis van de Wbp bepaald dat een organisatie die (bijzondere) persoonsgegevens verwerkt via haar website, de gehele webapplicatie via HTTPS moet aanbieden. Binnen de overheid is het gebruik van HTTPS in bepaalde gevallen verplicht. Organisaties die gebruik maken van Logius-diensten zoals DigiD en eHerkenning zijn bijvoorbeeld verplicht om vanaf de inlogpagina de website te beveiligen met HTTPS.

Metingen van het Forum Standaardisatie (medio 2016) laten zien dat voor bijna 80 procent van de overheidswebsites gebruik maakt van HTTPS. Slechts de helft hiervan volgde daarbij de aanbevelingen van het NCSC voor veilige TLS-configuratie. Het gebruik van HSTS is één keer gemeten voor gemeentelijke websites; bij ongeveer 65 procent van de gemeentelijke websites werd HSTS toegepast. Opvallend is dat met name landingspagina's vaak onbeveiligd zijn. Dit is een risico, aangezien bezoekers vanaf dit punt op de website doorklikken naar persoonlijke onderdelen (zoals contactformulieren of persoonlijke portalen) en mogelijk onopgemerkt worden geleid naar een andere, malafide website.

De grote browsers attenderen bezoekers van websites in toenemende mate actief of websites beveiligd zijn of niet. Dit draagt bij aan de bewustwording van veilig webverkeer.

Opname bevordert de adoptie
Hoewel de toepassing van HTTPS in combinatie met HSTS voor de beveiliging van websites toeneemt, heeft het gebruik nog niet de omvang die nodig is. De 'pas toe of leg uit'-lijst is het geschikte middel om de adoptie van HTTPS en HSTS te bevorderen. De verplichte status stimuleert tevens de adoptie van de standaard in aanloop naar de (mogelijke) verplichting van HT TPS na invoering van de Wet generieke digitale infrastructuur (GDI).

Toelichting van eventuele risico's
Er zijn geen specifieke risico's geïdentificeerd.

4. Wat is de conclusie van de consultatie?

Eventuele aanvullingen vanuit de consultatie
Op de openbare consultatie van het expertadvies zijn reacties ontvangen van IBD, Logius, CIBO, DICTU en Bas Meijer.

IBD
IBD heeft opmerkingen gemaakt over:
1. De behoefte om concreet te maken welke partijen de wens hebben om HTTPS te verplichten voor alle overheidswebsites en het functioneel toepassingsgebied te herformuleren.
   Reactie: bij het opstellen van het expertadvies is met meerdere organisaties gesproken en hen is gevraagd of zij het belang van de verplichting van HTTPS en HSTS onderschrijven. De verplichting van HTTPS en HSTS voor alle overheidswebsites en webservices maakt dat ook het functioneel toepassingsgebied opnieuw geherformuleerd moet worden.
2. Het gegeven dat het beveiligen tegen statelijke actoren bijna onmogelijk is, en dat met dit advies mogelijk een te positief beeld wordt gegeven.
   Reactie: voor het Forumadvies is gekozen om het beveiligen tegen statelijke actoren niet op te nemen.
3. Gebruikers eindverantwoordelijk zijn voor hun gedrag op het internet. Er zou volgens het IBD meer aandacht moeten worden besteed aan de bewustwording

van de gebruikers, zodat deze ook niet verder gaan bij een onveilige website of eerst onderzoek uitvoeren alvorens zij verder gaan.
Reactie: het Forum Standaardisatie vindt bewustwording belangrijk. In de adoptiestrategie wordt dit als aandachtspunt meegenomen. Dit is tevens een belangrijk aandachtspunt voor de (koepel)organisaties zelf.

4. In het expertadvies zou met name gesproken worden over het draagvlak van HTTPS, en niet van HSTS.
Reactie: dit is niet het geval. Ook heeft het Forum Standaardisatie nog maar één keer, en met beperkte scope, het gebruik van HSTS gemeten. Hierdoor is nog niets te zeggen over de veranderingen in het gebruik van HSTS.
5. Het organiseren van (veilig) certificaatbeheer. Het IBD is van mening dat dit in het expertadvies onderbelicht is.
Reactie: Certificaten(beleid) valt niet binnen de scope van deze experttoetsing. Het vertrouwen in de domeinnaam is echter wel belang. Het dient de aanbeveling om goed certificatenbeleid en (rijks)domeinnamen-beleid te hanteren. Voor het inrichten van het certificaatbeheer kan gebruik worden gemaakt van de factsheet 'Veilig beheer van digitale certificaten' van het NCSC.[3]

In de opmerkingen van IBD wordt geen reden gezien om het expertadvies te herzien of om aanvullende adviezen te geven.

Logius
Logius heeft opmerkingen gemaakt over:

1. De wens om het gebruik de standaard binnen 'webservices' te verduidelijken. Dit kan zowel om 'server to server' als 'server to client' gaan.
Reactie: Dit is aangepast in de toelichting op het functioneel toepassingsgebied. Het gaat alleen om 'server to client'.
2. Het belang van het opvolgen van de adviezen van het NCSC. Logius is van mening dat dit een directe plaats dient te hebben in het beveiligingsproces van elke organisatie.
Reactie: Het Forum Standaardisatie onderschrijft de waarde van de adviezen en richtlijnen van het NCSC. Waar relevant wordt bij standaarden die geplaatst zijn op de lijst met open standaarden verwezen naar de richtlijnen en adviezen van het NCSC.
3. Het advies om HTTP op te nemen in HTTPS en HSTS op de 'pas toe of leg uit'-lijst. Logius is van mening dat de status 'aanbevolen' kan worden behouden.
Reactie: met het verplichten van HTTPS is de plaatsing van HTTP op de aanbevolen lijst overbodig geworden. Omdat dit kan zorgen voor onduidelijkheid is er voor gekozen om HTTP te noemen in de toelichting op de website bij HTTPS en HSTS, maar hier geen formele status aan te verbinden.
4. Bij het ontwikkelen van 'toepassingsprofielen' op standaarden is het relevanter om een profiel te ontwikkelen dat voorschrijft hoe verschillende standaarden in samenhang worden gebruikt, dan om per standaard een profiel op te stellen.
Reactie: Bij de toetsing van standaarden wordt altijd getoetst of toepassingsprofielen noodzakelijk zijn voor het gebruiken van de standaard(en). Voor de implementatie HTTPS en HSTS zijn echter geen aanvullende profielen nodig.

In de opmerkingen van Logius wordt geen reden gezien om het expertadvies te herzien of om aanvullende adviezen te geven.

[3] *https://www.ncsc.nl/actueel/factsheets/factsheet-veilig-beheer-van-digitale-certificaten.html.*

CIBO
CIBO heeft opmerkingen gemaakt over:
1. Het gebruik van Extended-certificaten en het vast stellen van minimale eisen, minimaal TLS 1.2, SHA 256 2048 bits sleutellengte.
   Reactie: TLS 1.2 is een verplichte standaard op de lijst met open standaarden. Minimale eisen aan sleutellengtes komen terug in de standaard ETSI TS 119 312, welke op dit moment ter consultatie ligt voor de status 'aanbevolen' op de lijst met open standaarden. Certificaten(beleid) valt niet binnen de scope van deze experttoetsing. Het vertrouwen in de domeinnaam is echter wel belang. Het dient de aanbeveling om goed certificatenbeleid en rijksdomeinnamen-beleid te hanteren. Voor het inrichten van het certificaatbeheer kan gebruik worden gemaakt van de factsheet 'Veilig beheer van digitale certificaten' van het NCSC.[4]
2. De nadruk in het expertadvies om de lijn van de Amerikaanse overheid te volgen. CIBO wil graag dat wordt uitgegaan wordt van de richtlijnen van bijvoorbeeld de Autoriteit Persoonsgegevens en het NCSC.
   Reactie: In het Forumadvies is de verwijzing naar de Amerikaanse overheid niet opgenomen. Het functioneel toepassingsgebied wordt echter niet aangepast.
3. De adoptie-impuls om alle overheidswebsites HTTPS en HSTS inclusief de veilige configuratie conform NCSC uiterlijk eind 2018 hebben ingevoerd (aanvulling op de bestaande adoptieimpuls van het Nationaal Beraad). CIBO is van mening dat deze datum te ver in de toekomst ligt, en pleit om HTTPS en HSTS met directe ingang te implementeren of uiterlijk 1 juli 2017.
   Reactie: <aanvullen na afstemming in het Forum Standaardisatie>

In de opmerkingen van CIBO wordt geen reden gezien om het expertadvies te herzien of om aanvullende adviezen te geven.

DICTU
DICTU heeft opmerkingen gemaakt over:
1. Dat beveiliging van HSTS werkt binnen de gestelde HSTS-verlooptijd.
   Reactie: de levensduur van HSTS-headers moet passen bij het gebruiksdoel van de website. Als adoptieadvies is aanvullend opgenomen dat websites met digitale dienstverlening, bijvoorbeeld door middel van DigiD dienen te overwegen om hun domein op een pre-loading lijst te plaatsen om te voorkomen dat de landingspagina via HTTP benaderd kan worden.
2. Het domeinnamenbeleid voor Rijksoverheden. DICTU vraagt zich af of het handig is om overheidsbreed domeinnamenbeleid op te stellen.
   Reactie: Certificaten(beleid) valt niet binnen de scope van deze experttoetsing. Het vertrouwen in de domeinnaam is echter wel belang. Het dient de aanbeveling om goed certificatenbeleid en (rijks)domeinnamen-beleid te hanteren. Voor het inrichten van het certificaatbeheer kan gebruik worden gemaakt van de factsheet 'Veilig beheer van digitale certificaten' van het NCSC.[5]

Bas Meijer
Bas Meijer heeft opmerkingen gemaakt over het ontbreken van HPKP als geplaatste standaard op de lijst met open standaarden.
Reactie: HPKP staat niet op de lijst met open standaarden. Recent is gekeken naar HPKP en de voorlopige conclusie is dat dit geen stabiele standaard is waar veel (implementatie)risico's aan gebonden zijn. Het is uiteraard mogelijk om HPKP aan te melden voor de toetsingsprocedure voor open standaarden.

[4] *https://www.ncsc.nl/actueel/factsheets/factsheet-veilig-beheer-van-digitale-certificaten.html.*
[5] *https://www.ncsc.nl/actueel/factsheets/factsheet-veilig-beheer-van-digitale-certificaten.html.*

In de opmerkingen van Bas Meijer wordt geen reden gezien om het expertadvies te herzien of om aanvullende adviezen te geven.

De volledige reacties van IBD, Logius, CIBO, DICTU en Bas Meijer zijn terug te vinden in bijlage 2 Overzicht reacties consultatie.

5. Welke additionele adviezen zijn er ten aanzien van de adoptie van de standaard?
Naar aanleiding van de expertgroep zijn er bij opname op de lijst met open standaarden de volgende oproepen ten aanzien van de adoptie van de standaard te doen:

1. Als adoptie-impuls af te spreken dat alle overheidswebsites HTTPS en HSTS inclusief de veilige configuratie conform NCSC uiterlijk eind 2018 hebben ingevoerd. Dit is een aanvulling op de bestaande adoptieimpuls van het Nationaal Beraad. Daarbij is afgesproken dat HTTPS voor eind 2017 moet zijn ingevoerd voor die overheidswebsites waar burgers en/of bedrijven gegevens invoeren (zoals in een contactformulier) of waarbij gegevens vooringevuld zijn.
2. Bij de opname op de 'pas toe of leg uit'-lijst de volgende oproepen te doen:
   - Aan NCSC om de ontwikkelingen rondom HTTPS en HSTS te volgen en de genoemde ICT-beveiligingsrichtlijnen te actualiseren wanneer hier aanleiding toe is. Daarnaast wordt het NCSC opgeroepen om de ICT-beveiligingsrichtlijnen ook in het Engels beschikbaar te maken.
   - Aan de minister van Binnenlandse Zaken en Koninkrijksrelaties om, na inwerkingtreding van de wet GDI, niet alleen HTTPS maar ook HSTS en de veilige configuratie conform NCSC in onderzoek te nemen voor verplichting via een algemene maatregel van bestuur (AMvB).
   - Aan overheden de aanbevelingen uit de NCSC-factsheet 'Veilig beheer van digitale certificaten' (2012) te volgen. Onderdeel van deze factsheet is ook de aanschaf van een extra set 'back up'-certificaten. Hierdoor kan de impact van een hack bij of faillissement van een CA, zoals bij DigiNotar, worden beperkt.
   - Aan Platform Internetstandaarden om meer toelichting en achtergrondinformatie te geven bij de test op Internet.nl. Hiervoor kan met onder andere KING/IBD samengewerkt worden. Zij krijgt regelmatig vragen van gemeenten over de testresultaten.
   - Aan het Forum Standaardisatie om de voortgang van de adoptie van HTTPS en HSTS inclusief de veilige configuratie conform NCSC te monitoren en hierover aan het Nationaal Beraad te rapporteren.
   - Overheden met websites met digitale dienstverlening, bijvoorbeeld door middel van DigiD, dienen te overwegen om hun domein op een pre-loading lijst te plaatsen om te voorkomen dat de landingspagina via HTTP benaderd kan worden.

De opgeroepen partijen worden gevraagd om één jaar na opname van de standaard over de voortgang op deze punten te rapporteren aan het Forum Standaardisatie.

Bijlage

- Expertadvies HTTPS en HSTS
- Overzicht reacties consultatie