Forum Standaardisatie

Expertonderzoek HTTPS en HSTS

Datum 24 februari 2017

Colofon

Projectnaam	Expertonderzoek HTTPS en HSTS
Versienummer	1.0
Locatie	Den Haag
Organisatie	Forum Standaardisatie Postbus 96810 2509 JE Den Haag forumstandaardisatie@logius.nl

Auteur	Jasmijn Wijn (Verdonck, Klooster & Associates)

Inhoud

Forumadvies & Managementsamenvatting

Aanleiding
Door het Forum Standaardisatie worden momenteel de standaarden HTTP (versie 1.1 en 2), HTTPS en HSTS aanbevolen. 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 gevolgd.

Dit benadrukt de noodzaak voor een onderzoek naar een mogelijke statuswijziging van HTTPS en HSTS, van aanbevolen naar verplicht ('pas toe of leg uit'). Onderdeel van de toets is ook om het functioneel toepassingsgebied van HTTPS en HSTS te herijken.

Advies aan het Forum Standaardisatie
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.

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

Organisatorisch werkingsgebied:
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 onderdeel te maken van de opname van HTTPS én HSTS. Het advies is om TLS te behouden op 'pas toe of leg uit'-lijst omdat deze standaard ook toegepast kan worden om andersoortige communicatie dan webverkeer te beveiligen.

Waar gaan de standaarden inhoudelijk over?
HTTPS, is een uitbreiding op het HTTP-protocol met als doel een veilige uitwisseling van gegevens met een website of webservice. Bij gebruik van

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.

HTTPS worden de gegevens versleuteld, waardoor het voor een buitenstaander, bijvoorbeeld iemand die afluistert, onmogelijk zou moeten zijn om te weten welke gegevens verstuurd worden. Voor de versleuteling maakt HTTPS gebruik van TLS; men noemt HTTPS ook wel "HTTP over TLS".

HSTS is een aan HTTPS complementaire standaard die ervoor zorgt dat de webclient (in de regel een webbrowser) bij elke terugkerend bezoek de website alleen via HTTPS benadert. Dit helpt man-in-the-middle-aanvallen te voorkomen.

Hoe scoren de standaarden op de toetsingscriteria?

Toegevoegde waarde
De Nederlandse overheid moet vertrouwelijke informatie beschermen tegen afluisteren door aanvallers, zoals criminele partijen en statelijke actoren. Hieronder valt ook de communicatie tussen overheidspartijen, tussen de overheid en bedrijven, en tussen overheden en burgers via websites en webservices.

Daarnaast is het belangrijk dat burgers en bedrijven bij het bezoeken van een overheidswebsite er zeker van kunnen zijn dat deze ook daadwerkelijk van de overheid is ('eigenaarschap') 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. Alle vormen van surfgedrag dienen als privé en gevoelig te worden beschouwd en moeten dus beveiligd worden.

Overheidsorganisaties zijn op dit moment zelf verantwoordelijk om te bepalen of hun website gevoelige informatie bevat. Het verplichten van HTTPS en HSTS voor alle websites en webservices voorkomt dat op basis van subjectiviteit beslissingen worden genomen over welke informatie gevoelig is en welke niet. De kosten om de standaarden technisch te implementeren en te onderhouden zijn doorgaans verwaarloosbaar in verhouding tot de totale kosten voor het beheren van een website.

Open standaardisatieproces
Het standaardisatieproces van IETF is voldoende open. 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.[2]

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.

[2] https://www.autoriteitpersoonsgegevens.nl/nl/nieuws/beveiliging-contactformulier-op-websites-fysiotherapeuten.

Volgens meting van Forum Standaardisatie maakte medio 2016 bijna 80 procent van de overheidswebsites gebruik van HTTPS en 40 procent volgde daarbij de aanbevelingen voor veilige TLS-configuratie van NCSC . Een eerste meting geeft aan dat rond de 65 procent van gemeentelijke websites ook HSTS ondersteunt. 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 webbrowsers bieden al vele jaren ondersteuning voor HTTPS en attenderen bezoekers van websites in toenemende mate actief of websites beveiligd zijn of niet. Browsers ondersteunen de nieuwe http-versie, HTTP/2, alleen voor HTTPS-websites; niet beveiligde websites worden niet via HTTP/2 weergegeven De zoekmachine van Google scoort websites die met HTTPS zijn beveiligd hoger dan onbeveiligde websites.. Alle moderne webserversoftware (zoals Apache, Nginx en Windows IIS) biedt goede ondersteuning voor HTTPS.

Opname bevordert 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 HTTPS na invoering van de Wet generieke digitale infrastructuur (GDI).

Adoptieadviezen
Het Forum Standaardisatie en het Nationaal Beraad wordt, in aanvulling op de opname van HTTPS en HSTS inclusief de veilige configuratie conform NCSC, geadviseerd om:

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 adoptie-impuls 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 voor ingevuld 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 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 om 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 die regelmatig vragen van gemeenten ontvangt 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.

Hoe is het proces verlopen?
Dit advies is tot stand gekomen door een onderzoek in de vorm van deskresearch en interviews met experts. HTTPS en HSTS zijn opnieuw getoetst aan de hand van de toetsingscriteria van het Forum Standaardisatie. Op basis van deskresearch is een eerste conceptadvies opgesteld. In de interviews zijn de bevindingen getoetst en aangevuld.

1 Doelstelling expertadvies

1.1 Achtergrond

Het gebruik van open standaarden voor betrouwbare gegevensuitwisseling en het voorkomen van vendor lock-in is een van de doelstellingen van de Nederlandse overheid. Dit beleid wordt herbevestigd in actieplan "Open overheid", de digitale agenda 2017 en de kabinetsreactie op het rapport Elias. Tevens is het opgenomen in het instellingsbesluit van het Forum Standaardisatie en is het gebruik van standaarden ook geborgd in de Generieke Digitale Infrastructuur en de verschillende architectuurkaders. Dit onderstreept de noodzaak van het zoveel mogelijk meenemen van open standaarden bij het ontwerpen of inkopen van informatiesystemen.

Een van de maatregelen om de adoptie van standaarden te bevorderen is het beheren van een lijst met open standaarden, die vallen onder het principe 'pas toe of leg uit' of 'aanbevolen'. Het Nationaal Beraad Digitale Overheid (hierna Nationaal Beraad) spreekt zich uit over de standaarden die op de lijst zullen worden opgenomen, onder andere op basis van een expertbeoordeling van de standaard. Het Nationaal Beraad wordt geadviseerd door het Forum Standaardisatie. Het Bureau Forum Standaardisatie ondersteunt beide instellingen.

1.2 Aanleiding onderzoek HTTPS en HSTS

HTTPS (RFC 2818), HSTS (RFC 6797) en TLS zijn opgenomen op de lijst met open standaarden. TLS kent de zwaardere pas toe of leg uit verplichting en HTTPS in combinatie met HSTS zijn aanbevolen standaarden. Gezien de raakvlakken tussen deze standaarden, HTTPS is in feite HTTP over TLS en HSTS dwingt HTTPS af, is in de praktijk het verschil in status van deze standaarden verwarrend voor organisaties. Hier heeft het Forum Standaardisatie verschillende vragen over ontvangen. Ook is er een toenemende roep om HTTPS te verplichten voor alle overheidswebsite, blijkt ook uit Kamervragen.[3]

Het Forum Standaardisatie heeft, naar aanleiding van deze signalen, de wens om meer duidelijkheid te geven door de status van HTTPS en HSTS te wijzigen naar 'pas toe of leg uit' (verplicht). Ook bestaat de wens om het functioneel toepassingsgebied van HTTPS en HSTS zo te formuleren dat HTTPS en HSTS in alle gevallen en voor alle overheidswebsites verplicht worden, en niet alleen voor websites met inlogmogelijkheid of uitwisselingsmogelijkheid. Het doel van dit advies is om, aan de hand van de toetsingscriteria, vast te stellen of HTTPS en HSTS 'pas toe of leg uit'-standaarden moeten worden, en zo ja, onder welke voorwaarden.

1.3 Aanpak

Dit advies is tot stand gekomen door een onderzoek in de vorm van deskresearch en interviews. HTTPS en HSTS zijn opnieuw getoetst aan de hand van de toetsingscriteria van het Forum Standaardisatie. Op basis van deskresearch is een conceptadvies opgesteld. In de interviews zijn de bevindingen getoetst en aangevuld.

In het onderzoek zijn de volgende personen geïnterviewd:

[3] http://www.nu.nl/internet/4399254/plasterk-wil-toch-beveiligde-verbinding-verplichten-alle-overheidssites.html.

Naam	Organisatie	Functie
John Stienen	Ministerie van BZK	Senior beleidsadviseur
Gino Laan	Ministerie van BZK	Senior beleidsadviseur
Marjolein Kostman	Ministerie van BZK	Beleidsmedewerker Regie- en Kaderstelling
Michiel Leenaars	NLnet Foundation en Internet Society Nederland	Directeur
Jochem van den Berge	PKIoverheid	Consultant
Douglas Skirving	PKIoverheid	Senior Security Consultant
Pieter Rogaar	NCSC	Senior adviseur cybersecurity
Jelle Attema	ECP	Adviseur
Jule Hintzbergen	IBD	Adviseur Informatiebeveiliging
Thomas de Haan	Ministerie van EZ	Senior beleidsmedewerker

1.4 Vervolg

Dit advies zal ten behoeve van een publieke consultatie openbaar worden gemaakt door het Bureau Forum Standaardisatie. De openbare consultatie vindt plaats van 24 februari tot 25 maart 2017. Iedereen kan gedurende de consultatieperiode op dit expertadvies reageren.

Het Forum Standaardisatie zal op basis van het advies en de relevante inzichten uit de openbare consultatie een advies aan het Nationaal Beraad opstellen. Het Nationaal Beraad besluit uiteindelijk op basis van het advies van het Forum of de status van HTTPS en HSTS wordt aangepast van 'aanbevolen' naar 'pas toe of leg uit', eventueel onder voorwaarden.

1.5 Leeswijzer

Hoofdstuk 2 beschrijft op hoofdlijnen de werking van HTTPS en HSTS en de relatie met andere standaarden. Ook wordt gekeken naar verplichtingen en adviezen die voor HTTPS gelden. Hoofdstuk 3 geeft het resultaat van de toetsing van HTTPS en HSTS aan de toetsingscriteria weer. In hoofdstuk 4 wordt het advies gegeven over de mogelijke aanpassing van de status van HTTPS en HSTS op de lijst met open standaarden.

2 Toelichting op de standaarden

2.1 Toelichting 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 de volgende aspecten:

- *Vertrouwelijkheid*: het versleutelen van verstuurde gegevens (encryptie)[4], 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.

Vertrouwelijkheid

Zonder het gebruik van HTTPS worden de gegevens die tussen de client en server worden uitgewisseld verzonden in leesbare tekst. Wanneer deze gegevens worden verzonden kan deze informatie relatief eenvoudig worden onderschept. Dit wordt ook wel een passieve aanval genoemd. 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. Wanneer HTTPS wordt gebruikt zijn gegevens versleuteld, waardoor het niet mogelijk is om, in het geval van onderschepping, de gegevens uit te lezen zonder eerst het encryptie-algoritme te kraken.

IP-adressen en domeinnamen worden niet versleuteld door HTTPS. Versleuteld verkeer houdt altijd nog metadata bij over openbaar beschikbare informatie, bijvoorbeeld het aantal megapixels van een foto of bites van een video. Op basis van deze informatie zou een aanvaller ook kunnen achterhalen welke pagina bezocht is.

Integriteit

Bij een onveilige verbinding is het mogelijk om bij de verzending van informatie deze aan te passen, waardoor valse/verkeerde informatie wordt verstuurd en weergegeven (actieve aanval). HTTPS beschermt de data zodat het niet gewijzigd of overrulled kan worden.

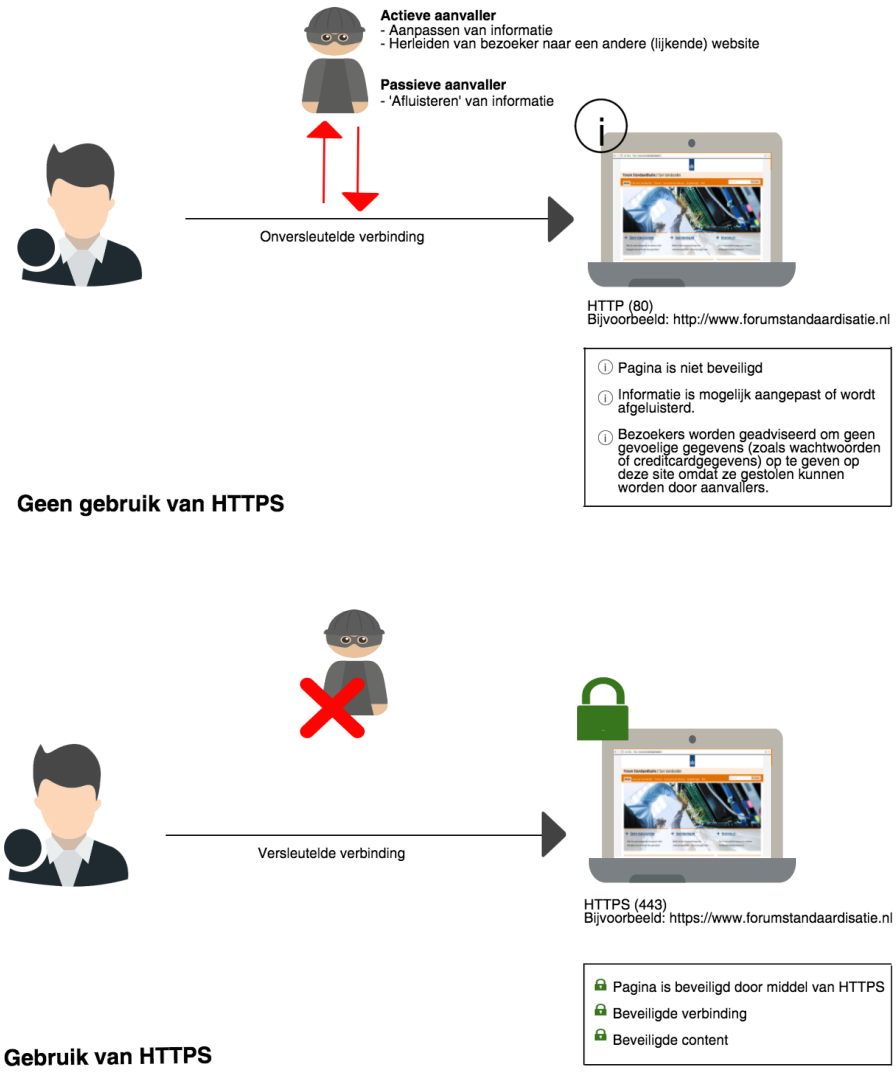
Authenticiteit

Bij het maken van een veilige verbinding naar een onbekende partij is een online controle op de identiteit van de verzendende partij en de eindbestemming wenselijk. Dit kan door middel van een (gepubliceerd) certificaat (een bestand met een digitale handtekening) dat door een certificaatautoriteit (CA) is uitgegeven of door een self-signed certificaat. Hiermee wordt gegarandeerd dat de 'public key' bij een bepaalde organisatie of persoon hoort. Het HTTPS-protocol dwingt af dat het

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

certificaat geverifieerd wordt voordat gegevens worden uitgewisseld. Indien dit niet mogelijk is zal de verbinding worden geblokkeerd en wordt de bezoeker van de website gewaarschuwd. Hierdoor is het niet mogelijk om een bezoeker van een website te herleiden naar een andere, lijkende website (actieve aanval). De verschillende certificaatniveaus worden kort toegelicht in de volgende paragraaf.

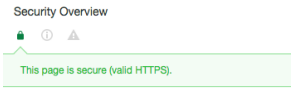
Zie figuur 1 voor een weergave van de functionaliteit van HTTPS voor websites.



Figuur 1. Weergave functionaliteit van HTTPS voor websites.

Omdat de gegevens aan beide kanten door een beveiligde verbinding gaan, moeten zowel de server als de client hun data versleutelen en ontcijferen. Vlak voor en na de versleuteling is de gegevensoverdracht identiek aan het HTTP-protocol.

Herkenbaarheid HTTPS voor bezoekers van een website
Bezoekers van een website kunnen een beveiligde verbinding met een website herkennen aan HTTPS in de URL (HTTPS://<EXAMPLE.NL>). De website-identiteitsknop (het hangslot) wordt in de adresbalk weergegeven zodra een bezoeker een beveiligde website bezoekt (zie figuur 2).

Veilig | https://	Beveiligde verbinding met de website en de pagina. Een bezoeker kan er zeker van zijn dat hij verbonden is met de website waarvan het adres in de adresbalk wordt weergegeven, dat de verbinding niet is onderschept en dat de informatie op de website niet is aangepast. Daarnaast is de verbinding versleuteld waardoor afluisteren wordt voorkomen. 
https://	Inhoud van de pagina is deels onbeveiligd. Bezoekers kunnen wel veilig gegevens invoeren en versturen, maar de informatie op de website kan door een derde zijn aangepast.
https://	Risicovolle, onbeveiligde inhoud op de website of er zijn problemen met het certificaat. Mogelijk heeft een derde de verbinding met de website gemanipuleerd. Bezoekers worden geadviseerd om geen gevoelige gegevens zoals wachtwoorden op te geven omdat ze gestolen kunnen worden.

Figuur 2. Weergave beveiligde, deels-beveiligde en niet-beveiligde verbinding met de website en pagina en toelichting website-identiteitsknop bij een beveiligde website.

2.2 Toepassing HTTPS in combinatie van 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 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.

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 preloading
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://<EXAMPLE.NL> 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.

2.3 HTTPS en TLS

Transport Layer Security (TLS) is een protocol dat tot doel heeft om beveiligde verbindingen over het internet te verzorgen. TLS biedt een beveiligde basis waar applicatieprotocollen zoals HTTP (voor webverkeer) of SMTP en IMAP (voor mailuitwisseling) op hun beurt weer op kunnen bouwen en gebruik van kunnen maken. Een HTTPS-verbinding is dus een TLS-verbinding met daarin een normale HTTP-verbinding. Het TLS-protocol is dus breder dan HTTPS.

TLS maakt gebruik van certificaten om zekerheid te bieden over de identiteit van een of beide communicerende partijen voordat communicatie plaatsvindt. Ook wordt met behulp van (het sleutelpaar van) de certificaten op betrouwbare wijze de encryptiesleutel uitgewisseld, die de standaard vervolgens gebruikt om met behulp van encryptietechniek beveiligde communicatie tussen partijen mogelijk te maken.

Toepassing van TLS
TLS wordt veelal gebruikt in situaties waarin het van belang is om vast te kunnen stellen of een gebruiker verbonden is met de juiste server of (overheids)website, zodat persoonlijke of vertrouwelijke informatie kan worden uitgewisseld. De toepassing van TLS is zodoende breder dan alleen de beveiligde verbinding met een website (HTTPS). Dit blijkt ook uit het vastgestelde functioneel toepassingsgebied:

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.

2.4 HTTPS in relatie tot HTTP/2

Hypertext Transfer Protocol (HTTP) is het protocol voor communicatie tussen een webclient (zoals een browser) en een webserver. Eind 2016 is door het Nationaal Beraad besloten om naast de 1.1-versie van HTTP ook de 2-versie toe te voegen aan de lijst met aanbevolen standaarden. HTTP/2[5] biedt ten opzichte van HTTP/1.1 meer en betere functionaliteit voor websites waar, ten behoeve van de gebruikerservaring, de snelheid van laden en het gebruiken van (interactieve) webpagina's van belang is.

[5] https://tools.ietf.org/html/rfc7540.

Het voordeel van HTTP/2 is dat browsers onbeveiligd HTTP/2-verkeer niet ondersteunen. De browsers dwingen zodoende het gebruik van HTTPS af. Dit benadrukt ook het belang van HTTPS voor webverkeer.

2.5 Verplichtingen en adviezen rondom HTTPS

In de loop der jaren zijn verschillende verplichtingen en adviezen voor informatiebeveiligingsstandaarden afgegeven. Hieronder worden kort de verplichtingen en adviezen beschreven die gelden voor HTTPS.

HTTPS als aanbevolen standaard op de lijst met open standaarden
Forum Standaardisatie
HTTPS (RFC 2818) is sinds 2009 als aanbevolen standaard opgenomen op de lijst met open standaarden van het Forum Standaardisatie. Het gebruik van HTTPS wordt aanbevolen voor de beveiligde uitwisseling van gegevens via het internet.

In 2016 is door het Forum Standaardisatie besloten om HSTS toe te voegen aan HTTPS. Het advies is om HTTPS altijd te gebruiken in combinatie met HSTS (RFC 6797[6] [7]). Als een website HSTS gebruikt zal de browser voor elke terugkerende bezoeker de website opnieuw via HTTPS aanbieden. Hierdoor zijn man-in-the-middle-aanvallen (MiM-aanvallen) bij terugkerende bezoekers niet mogelijk.

Adoptie impuls Informatiebeveiligingsstandaarden
Nationaal Beraad
Het Nationaal Beraad heeft op 18 mei 2015[8] op advies van het Forum Standaardisatie een adoptie-impuls (streefbeeld) uitgesproken voor de informatiebeveiligingsstandaarden TLS, DKIM, DMARC, DNSSEC en SPF. Met deze adoptie-impuls wordt er naar gestreefd dat deze standaarden uiterlijk eind 2017 bij alle overheidsorganisaties, binnen de vastgestelde organisatorisch toepassingsgebieden en voor het vastgestelde toepassingsgebied, geïmplementeerd zijn. Voor TLS (en dus HTTPS) houdt dit concreet in dat de standaard eind 2017 op alle overheidswebsites met gevoelige gegevens of een inlog/transactiemogelijkheid geïmplementeerd moet zijn.

Adoptieafspraak TLS/HTTPS
Nationaal Beraad
Voor TLS/HTTPS heeft het Nationaal Beraad in 2016 de adoptieafspraak gemaakt 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 voor ingevuld zijn.

Algemene maatregel van bestuur voor verplichting HTTPS (aankomend)
Ministerie van Binnenlandse Zaken en Koninkrijksrelaties (BZK)
Begin 2017 heeft minister Plasterk van Binnenlandse Zaken aangegeven na de invoering van de Wet generieke digitale infrastructuur (Wet GDI) HTTPS voor alle overheidswebsites te willen verplichten. Aangezien het gaat om verplicht van standaarden die staan op de 'ptolu'-lijst benadrukt dit de noodzaak voor het onderzoek naar de mogelijke statuswijziging van

[6] https://datatracker.ietf.org/doc/rfc2818/.
[7] https://tools.ietf.org/html/rfc6797.
8 https://digitaleoverheid.pleio.nl/file/download/41685652

HTTPS en HSTS.[9] Overigens wordt bij het instellen van een AMvB op basis van de Wet GDI een aparte consultatie gehouden.

Advies gebruik en configuratie van HTTPS
NCSC
Het NCSC adviseert om alle websites die gevoelige gegevens verwerken te beschermen met HTTPS. In de meting Informatiebeveiligingsstandaarden van het Forum Standaardisatie wordt het gebruik van TLS binnen overheden gemeten conform de richtlijnen van het NCSC. [10] Aanvullend adviseert het NCSC om HSTS, forward secrecy of SHA-2 (HTTPS-opties) te gebruiken bij alle websites die met HTTPS beveiligd zijn.[11] Het advies is dan ook om HTTPS i.c.m. HSTS te verplichten conform de configuratie van NCSC.

Norm ICT-beveiligingsassessments DigiD
Logius
De Norm ICT-beveiligingsassessments DigiD is bedoeld voor organisaties die DigiD gebruiken en jaarlijks een ICT-beveiligingsassessment moeten doen. De norm is gebaseerd op de *ICT-beveiligingsrichtlijnen voor webapplicaties* van het NCSC. In deze richtlijn wordt het gebruik van versleutelde (HTTPS) verbindingen verplicht gesteld voor websites die DigiD aanbieden.[12]

Beveiligingsnorm Wet bescherming persoonsgegevens (Wbp)
Autoriteit Persoonsgegevens
De Wbp vereist dat de verantwoordelijke passende technische en organisatorische maatregelen neemt om persoonsgegevens te beveiligen tegen verlies of tegen enige vorm van onrechtmatige verwerking (Wbp, art.13, lid). Om te bepalen wat 'passende maatregelen' zijn baseert de Autoriteit Persoonsgegevens zich onder andere op de ICT-ICT-Beveiligingsbeveiligingsrichtlijnen Webapplicaties van het NCSC. In een brief aan de KNGF, de overkoepelende vereniging van fysiotherapeuten, heeft de Autoriteit Persoonsgegevens toegelicht hoe om te gaan met gegevens op websites:

Indien via een contactformulier op de website bijzondere persoonsgegevens – waaronder gezondheidsgegevens en BSN – worden verwerkt, dient de gehele webapplicatie via HTTPS te worden aangeboden.

Indien uitsluitend andersoortige gegevens worden verwerkt dan moet de organisatie zelf op basis van een risicoanalyse en classificatieschema vaststellen of de webapplicatie via HTTPS wordt aangeboden.[13]

2.6 Relatie met andere standaarden

HTTPS werkt goed samen met de gangbare internetprotocollen en internettechnologie zoals het eerder genoemde HTTP, TLS en HSTS. HTTPS werkt ook goed samen met protocollen als SAML en SOAP.

[9] http://www.nu.nl/internet/4399254/plasterk-wil-toch-beveiligde-verbinding-verplichten-alle-overheidssites.html.
[10] ICT-Beveiligingsrichtlijnen voor Webapplicaties, september 2015 en ICT-Beveiligingsrichtlijnen voor Transport Layer Security (TLS), november 2014.
[11] Factsheet FS-2014-03 *HTTPS kan een stuk veiliger. Controleer configuraties en pas nieuwe opties toe*, november 2014.
[12] https://www.logius.nl/fileadmin/logius/ns/diensten/digid/assessments/20161215_norm_V2_ict-beveiligingsassessments_digid.pdf.
[13] https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/brief_aan_kngf.pdf.

3 Toetsing van HTTPS aan criteria

Om te bepalen of een standaard opgenomen moet worden op de lijst met open standaarden wordt deze getoetst aan een aantal criteria. Er zijn vier hoofdcriteria:

1. Toegevoegde waarde
2. Open standaardisatieproces
3. Draagvlak
4. Opname bevordert adoptie

Deze criteria staan beschreven in het rapport, *"Toetsingprocedure en criteria voor lijst met open standaarden, voor indieners en experts"* en staan op de website https://www.forumstandaardisatie.nl/content/aanmelden-en-beheren-van-standaarden.

Voor dit onderzoek is HTTPS getoetst aan deze criteria. Het resultaat van de toetsing is in dit hoofdstuk per criterium beschreven. Voor de volledigheid is tevens de definitie van elk criterium opgenomen.

3.1 Toegevoegde waarde

De interoperabiliteitswinst en andere voordelen van adoptie van de standaard wegen overheidsbreed en maatschappelijk op tegen de risico's en nadelen.

HTTPS is algemeen toepasbaar, ook binnen het werkgebied van de (semi-)overheid. HTTPS wordt gebruikt om webverkeer te beschermen tegen onbevoegde partijen die mee willen lezen (passieve aanvallers) of het webverkeer willen manipuleren (actieve aanvallers). Op dit moment wordt de standaard veel gebruikt bij betalingstransacties en bij de uitwisseling of verzending en opslag van persoonsgegevens zoals naam, adres en geboortedatum. Dit is ook conform de verplichting vanuit de Wbp.

Zoals ook opgenomen in het instellingsbesluit staat het Forum voor betrouwbare berichtenuitwisseling. Dit is belangrijk omdat met de toenemende digitalisering van de overheid ook de dreiging van digitale aanvallen toeneemt. Door middel van digitale (economische) spionage kan in een kort tijdsbestek grote hoeveelheden informatie op grotendeels anonieme en simultane wijze worden verzameld. Ook kan informatie worden aangepast. De Nederlandse overheid moet vertrouwelijke informatie beschermen tegen afluisteren door aanvallers, zoals criminele partijen en statelijke actoren. Hieronder valt ook de communicatie tussen overheidspartijen, tussen de overheid en bedrijven, en tussen overheden en burgers. Daarnaast is het belangrijk dat burgers en bedrijven bij het bezoeken van een overheidswebsite er zeker van kunnen zijn dat deze ook daadwerkelijk van de overheid is (eigenaarschap) en dat informatie niet is aangepast of kan worden afgeluisterd/aangepast.

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. Voor bestaande websites geldt dat de website gemigreerd moet worden naar HTTPS, inclusief de aanpassing van alle links naar bestaande (wellicht deels uit externe bronnen) geïncorporeerde content . Nieuwe websites kunnen gelijk geheel op basis van HTTPS worden gebouwd.

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.

De kosten van het aanschaffen en beheren van een HTTPS-certificaat is ongeveer € 600,00 per organisatie. De implementatie van HTTPS kan kosteloos op een aantal websites worden getest, zoals https://internet.nl. De geldigheid en scope van de certificaten (zie paragraaf 2.2) kan getest worden op https://www.ssllabs.com/index.html en via OWASP.

3.2 Open standaardisatieproces

De ontwikkeling en het beheer van de standaard zijn op een open, onafhankelijke, toegankelijke, inzichtelijke, zorgvuldige en duurzame wijze ingericht.

HTTPS (RFC 2818)[14] en HSTS (RFC 6797)[15] worden beheerd door de internationale beheerorganisatie Internet Engineering Task Force (IETF).

IETF is onafhankelijk, kent goed gedocumenteerde en open beheerprocedures. Er is geen lidmaatschap, het beheren en de besluitvorming hieromtrent is open en transparant en partijen kunnen zich hiervoor aanmelden. Documentatie over de standaarden is kosteloos verkrijgbaar. De financiering van de ontwikkeling en het onderhoud van de standaarden wordt verzorgd door de leden van de werkgroep waar de standaard onder valt. IETF bestaat ruim 30 jaar en heeft zich in het verleden bewezen als stabiele standaardisatieorganisatie.

Specificaties doorlopen in het standaardisatieproces van IETF twee stadia van volwassenheid: ‘proposed standard’ en ‘internet standard’. De voortgang van de standaard in dit proces is transparant en kosteloos te volgen via de website van IETF. HTTPS, als toepassing van TLS, en HSTS zijn, net als TLS, STARTTLS en DANE, proposed standards. RFC 2818 (HTTPS) is sinds de publicatie in 2000 inhoudelijk niet meer gewijzigd, RFC 6797 (HSTS) is sinds 2012 niet meer gewijzigd.

[14] https://tools.ietf.org/html/rfc2818.
[15] https://tools.ietf.org/html/rfc6797.

3.3 Draagvlak

Aanbieders en gebruikers moeten voldoende ervaring hebben bij het ondersteunen, implementeren en gebruiken van de standaard.

Gebruik
De standaard wordt in Nederland veel gebruikt bij websites waarbij betalingstransacties, inloggen en de uitwisseling of verzending en opslag van privacygevoelige informatie zoals naam, adres, geboortedatum en andere persoonsgegevens plaatsvindt.

Binnen de overheid is het gebruik van versleutelde verbindingen voor specifieke websites en services verplicht. Organisaties die gebruik maken van Logius-diensten zoals DigiD zijn bijvoorbeeld verplicht om vanaf de inlogpagina de website te beveiligen met HTTPS. Enkele voorbeelden van organisaties die gebruik maken van Logius-diensten zijn DUO, Belastingdienst en gemeenten die digitale dienstverlening aanbieden. Maar ook overheidswebsites met publieke informatie maken in toenemende mate gebruik van HTTPS. Dienst Publiek en Communicatie van het ministerie van Algemene Zaken heeft bijvoorbeeld alle 200+ websites op het Platform Rijksoverheid Online (o.a. rijksoverheid.nl, defensie.nl) beschermd met HTTPS, en het CBS gebruikt op zijn publieke website cbs.nl ook HTTPS.

Uit meting van van het Forum Standaardisatie is gebleken dat ongeveer 4 van de 5 overheidswebsites TLS ondersteunen.[16] HTTPS werd in 2016 bij bijna 80 procent van de overheidswebsites (zowel centraal als decentrale overheden) gebruikt.. Het gebruik van TLS voor websites conform de aanbevelingen van het NCSC is tussen vanaf 2015 tot medio 2016 gestegen van 6 naar 40 procent. Het gebruik van HSTS is recent gemeten bij gemeenten. HSTS wordt door ongeveer de 65% van de gemeentelijke websites ondersteund.

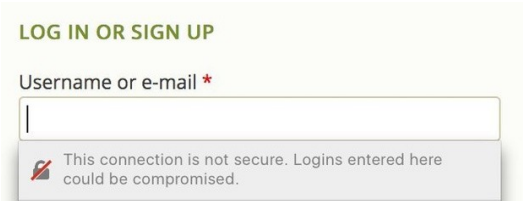
Opvallend is dat niet alle websites c.q. pagina's van overheidswebsites beveiligd zijn door middel van HTTPS. Landingspagina's zijn vaker onbeveiligd. Wanneer een gebruiker vervolgens navigeert naar een inlogpagina of een bestelformulier dan wordt er doorgelinkt naar een met HTTPS-beveiligde omgeving. Dit garandeert echter niet dat een bezoeker wordt doorgelinkt naar een andere (malafide) website dan initieel de bedoeling was.

De Amerikaanse overheid verplicht sinds 1 januari 2017 het gebruik van HTTPS voor alle websites van de federale overheid die voor het publiek toegankelijk zijn. Het uitgangspunt hierbij is dat alle vormen van surfgedrag als privé en gevoelig wordt beschouwd, en dus beveiligd moet worden. Hierdoor wordt voorkomen dat op basis van subjectiviteit beslissingen worden genomen over welke informatie gevoelig is en welke informatie niet.

Mozilla heeft op basis van een steekproef met gegevens van gebruikers van Firefox geconcludeerd dat eind 2016 meer dan 50 procent van de opgevraagde webpagina's beveiligd waren door middel van HTTPS.

[16] *https://www.forumstandaardisatie.nl/sites/bfs/files/proceedings/FS%20161214.4A%20Concept%20Monitor%20OSB%202016.pdf.*

Ondersteuning door leveranciers
De grote webbrowsers zoals Chrome, Internet Explorer, Firefox en Safari laten zien of een website een beveiligde verbinding tot stand brengt en geeft hierbij een toelichting/advies (zie paragraaf 2.1). Mozilla (Firefox) en Google (Chrome) willen aanvullend een waarschuwing geven wanneer een bezoeker wil inloggen op een onbeveiligde website (zie figuur 3).



Figuur 3. Waarschuwing bij een inlogpagina van een website die niet beveiligd is met HTTPS.

Zoals eerder aangegeven dwingen browsers het gebruik van HTTPS af via HTTP/2. Websites die geen HTTPS gebruiken worden geblokkeerd en niet via http/2 weergegeven voor bezoekers. Google plaatst websites die HTTPS gebruiken hoger in de zoekresultaten dan niet beveiligde websites (HTTP). Beveiligde websites hebben op deze manier een streepje voor op onbeveiligde websites.

Het Platform Internetstandaarden meet sinds 2016 ook 'afgedwongen HTTPS'. Geïnteresseerden kunnen de beveiliging van websites op het gebruik van onder andere HTTPS controleren op https://internet.nl en https://pulse.openstate.eu/https/domains/.

Alle grote webservers zoals Apache, Ngix en IIS ondersteunen HTTPS. Dit geldt ook voor load balancers.

3.4 Opname bevordert adoptie

De opname op de lijst is een geschikt middel om de adoptie van de standaard te bevorderen.

Er zijn twee lijsten: de lijst met gangbare standaarden en de lijst voor 'pas toe of leg uit'. Deze laatste lijst is bedoeld om standaarden een extra stimulans te geven wanneer:
1. Hun huidige adoptie binnen de (semi-)overheid beperkt is;
2. Opname bijdraagt aan de adoptie door te stimuleren o.b.v. het 'pas toe of leg uit' regime.

De lijst met gangbare standaarden vormt een referentie voor standaarden die veel gebruikt worden. Als standaarden voldoen aan enkele basisvoorwaarden (voor o.a. openheid), er is geen discussie over en de standaarden worden breed gebruikt, dan vindt opname op die lijst plaats.

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 om de standaard als gangbaar te kunnen beschouwen. 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 een (mogelijk) verplichting van HTTPS na invoering van de Wet generieke digitale infrastructuur (GDI).

4 Advies

4.1 Noodzaak voor de verplichting van HTTPS en HSTS

De noodzaak voor de verplichting van HTTPS en HSTS kan zowel vanuit het perspectief van overheden (als eigenaar van websites) als vanuit het perspectief van burgers en bedrijven (als bezoeker van websites) worden bekeken.

Overheden als eigenaar van websites

Met de toenemende digitalisering van de overheid worden steeds meer gegevens uitgewisseld. Hierdoor neemt ook de dreiging van aanvallen toe. In een kort tijdsbestek kunnen grote hoeveelheden informatie op grotendeels anonieme en simultane wijze worden verzameld en/of aangepast. De Nederlandse overheid moet vertrouwelijke informatie beschermen tegen afluisteren door aanvallers, zoals criminele partijen en statelijke actoren. Hieronder valt ook de communicatie tussen overheidspartijen, tussen de overheid en bedrijven, en tussen overheden en burgers. De definitie van *vertrouwelijke informatie* is echter ambigue, de beoordeling van vertrouwelijkheid is subjectief. Organisaties zijn zelf verantwoordelijk om te beoordelen of hun website gevoelige informatie bevat. Het verplichten van HTTPS en HSTS voor alle overheidswebsites zorgt er voor dat deze afzonderlijk beoordeling niet meer nodig en niet meer relevant is.

Hier wordt het uitgangspunt van de Amerikaanse overheid overgenomen: *alle vormen van surfgedrag worden als privé en gevoelig beschouwd, en moet dus beveiligd worden.*

Ook moet voorkomen worden dat bezoekers van een overheidswebsite ongemerkt door derden omgeleid kunnen worden naar een andere pagina omdat zij vanuit een onbeveiligde landingspagina doorklikken op de website.

Burgers en bedrijven als bezoekers van websites

Wanneer een overheidswebsite geen HTTPS en HSTS gebruikt ligt de verantwoordelijkheid voor het verantwoord gebruik van de (mogelijkheden van de) website bij de bezoeker van de website. De overheid moet er naar streven om bezoekers van website zo veilig mogelijk informatie te geven en gegevens in te vullen.

Burgers en bedrijven moeten in staat worden gesteld om vertrouwelijk te communiceren met de overheid. Burgers en bedrijven moeten bij het bezoeken van een overheidswebsite er zeker van kunnen zijn dat deze ook daadwerkelijk van de overheid is (eigenaarschap) en dat informatie niet is aangepast of kan worden afgeluisterd.

4.2 Functioneel toepassingsgebied en organisatorisch werkingsgebied

Functioneel toepassingsgebied
Huidige formulering functioneel toepassingsgebied van HTTPS en HSTS is:
Beveiligde uitwisseling van gegevens via het web.

Deze beschrijving is weinig specifiek en erg breed. Op basis van onderliggend onderzoek kan geconcludeerd worden dat het wenselijk is om HTTPS en HSTS voor alle overheidswebsites te verplichten. Als nieuw functioneel toepassingsgebied wordt voorgesteld:
Het beveiligen van de communicatie tussen clients (zoals webbrowsers) en servers voor alle via internet benaderbare websites en -webservices.

Aanvullend wordt geadviseerd om ook de intranetten van (semi-) overheidsorganisaties te beveiligen met HTTPS.

Organisatorisch werkingsgebied
Geadviseerd wordt om het organisatorisch werkingsgebied van HTTPS en HSTS overeen te laten komen met het werkingsgebied waarop het 'pas toe of leg uit'-principe van toepassing is, te weten:
Nederlandse overheden (Rijk, provincies, gemeenten en waterschappen) en instellingen uit de (semi-)publieke sector.

4.3 Adoptieactiviteiten

Gebruik van de standaard is het einddoel van het Forum en Nationaal Beraad. Plaatsing op de lijsten is hiervoor een goede stap, maar voor het daadwerkelijk adopteren (implementeren en gebruiken) van de standaard is vaak aanvullende actie benodigd. Aanvullend kan Forum Standaardisatie dan ook bijdragen aan adoptie van de standaard door het actief inzetten van adoptie-instrumenten of ondersteunende acties. Welke kansen zijn er om de adoptie te versnellen en welke drempels bestaan er die de adoptie van de standaard hinderen?

Het Forum Standaardisatie en het Nationaal Beraad wordt, in aanvulling op de opname van HTTPS en HSTS inclusief de veilige configuratie conform NCSC, geadviseerd om:

1. als adoptie-impuls af te spreken dat alle overheidswebsites HTTPS en HSTS inclusief de veilige configuratie conform NCSC hebben ingevoerd voor eind 2018. Dit is een aanvulling op de bestaande adoptie-impuls 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 voor ingevuld 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 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 om 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 die regelmatig vragen van gemeenten ontvangt 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.