Forum Standaardisatie

Wilhelmina van Pruisenweg 52
2595 AN Den Haag

Postbus 96810
2509 JE Den Haag

www.forumstandaardisatie.nl

notitie

Aan:	Forum Standaardisatie		
Van:	Bureau Forum Standaardisatie		
Datum:	28 maart 2017	**Versie**	1.0
Betreft:	Overzicht reactie openbare consultatieronde HTTPS & HSTS		
Bijlagen:	1. Reactie John van Huijgevoort, IBD 2. Reactie Peter Leijnse, Logius 3. Reactie John-Paul Kloosterman, CIBO 4. Reactie Friso van der Kreeft, DICTU 5. Reactie Bas Meijer		

Datum
28 maart 2017

1. Reactie IBD

Van: John van Huijgevoort - IBD
Verzonden: maandag 27 maart 2017 16:43
Aan: Jasmijn Wijn
Onderwerp: Aanmelden van standaarden en Reminder openbare consultatie

Dag Jasmijn,

Hierbij het juiste consultatiedocument met de opmerkingen van de IBD. De opmerkingen in het expertadvies blijven uiteraard ook nog van toepassing.

Succes.

Met vriendelijke groet,

John van Huijgevoort
Adviseur Informatiebeveiliging

Vragen over hoofdstuk 1 "Doelstelling expertadvies"

1. Zijn er volgens u in deze toelichting aanvullingen of anderszins wijzigingen nodig in paragraaf 1.2 en 1.3 ('Aanleiding onderzoek HTTPS en HSTS' en 'Aanpak') bezien vanuit het doel van het document (het Forum en Nationaal Beraad Digitale Overheid voorzien van een inhoudelijk relevante toelichting)? **Ja er worden nu termen gebruikt als 'Ook is er een toenemende roep om HTTPS te verplichten voor alle overheidswebsite' en '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', zonder dat wordt aangegeven waarop dit is gebaseerd. Maak dit concreet naam en toenaam vermelden.**

Vragen over hoofdstuk 2 "Toelichting op de standaarden"

2. Zijn er volgens u in deze toelichting aanvullingen of anderszins wijzigingen nodig in hoofdstuk 2 ('Toelichting op de standaarden) bezien vanuit het doel van het document (het Forum en Nationaal Beraad Digitale Overheid voorzien van een inhoudelijk relevante toelichting?
   Par 2.1:
   Er wordt nu gesteld dat '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 eindverantwoordelijkheid ligt echter bij de gebruiker en die zal bewust gemakt dienen te worden dat deze dan ook niet verder gaat maar stopt of nader onderzoek uitvoert om vast te stellen of het toch veilig is.

Vragen over hoofdstuk 3 "Toetsing van HTTPS aan de criteria"

3. Bent u het eens met de constateringen en conclusies inzake de toegevoegde waarde? [paragraaf 3.1 van het expertadvies]? **Er wordt nu gesteld '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.'

Natuurlijk dient de Nederlandse overheid de gegevens te beschermen, maar recente berichten hebben aangetoond dat het beveiligen tegen statelijke actoren (USA, Rusland, etc.) bijna onmogelijk is. Dus dit is meer bangmakerij, lijkt mij! Wat nuanceren en wellicht verwijzen naar het CSBN 2016.

Het zijn natuurlijk niet alleen de kosten voor de aanschaf van een certificaat maar ook nog de beheerkosten. Zie hiervoor de factsheet TLS van de Informatiebeveiligingsdienst voor gemeenten (IBD).

4. Bent u het eens met de constateringen en conclusies inzake het open standaardisatieproces? [paragraaf 3.2 van het expertadvies]? **Geen opmerkingen.**

5. Bent u het eens met de constateringen en conclusies inzake het draagvlak? [paragraaf 3.3 van het expertadvies]? **Het draagvlak gaat alleen maar over HTTPS en niet over HSTS.**

   Ik zou de alinea '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.' Verplaatsen naar toegevoegde waarde i.p.v.draagvalk.

   Nu is het voorbeeld dat de Amerikaanse overheid sinds 1 januari 2017 het gebruik van HTTPS voor alle websites van de federale overheid die voor het publiek toegankelijk zijn verplicht, wellicht niet het beste voorbeeld gezien de publicaties via Wikileaks en Snowden over de backdoors waarover de Amerikaanse overheid beschikt!

6. Bent u het eens met de constateringen en conclusies inzake de bevordering van de adoptie door opname op de lijst? [paragraaf 3.4 van het expertadvies]? **Geen opmerkingen.**

Vragen over het advies aan het Forum

7. Bent u het eens met de beredenering en conclusie inzake de noodzaak voor de verplichting van HTTPS en HSTS? [paragraaf 4.1 van het expertadvies] **Geen opmerkingen.**

8. Bent u het eens met het geadviseerde functioneel toepassingsgebied en organisatorisch werkingsgebied? [paragraaf 4.2 van het expertadvies] **Geen opmerkingen.**

9. Bent u het eens met de adoptie-aanbevelingen aan het Nationaal Beraad Digitale Overheid? [paragraaf 4.3 van het expertadvies] **Geen opmerkingen.**

Resterende inhoudelijke opmerkingen

10. Is/zijn er volgens u nog andere informatie of overwegingen die aan het Forum en Nationaal Beraad Digitale Overheid zou moeten worden meegegeven voor een besluit over het opnemen van deze standaard op de 'pas toe of leg uit'-lijst?
    Een belangrijk aspect is het organiseren van het certificaatbeheer. Dat wordt nu onderbelicht. Naast het 'juist' configureren van TLS dient de gemeente een digitaal certificaat aan te vragen bij een CA. Een gemeente dient een eigen afweging te maken welk type certificaat voor welke dienstverlening noodzakelijk is. Zie hiervoor het onderdeel digitale certificaten in deze factsheet. Voor het inrichten van het certificaatbeheer kunnen gemeenten gebruik maken van de factsheet 'Veilig beheer van digitale certificaten' van het NCSC.

Datum
28 maart 2017

2. Reactie Logius

Van: Leijnse, P (Peter) - Logius
Verzonden: vrijdag 24 maart 2017 15:22
Aan: Forum standaardisatie
Onderwerp: Consultatie HTTPS/HSTS en OAuth 2.0

Beste collega,

Bijgaand de reactie vanuit Logius op de consultaties van HTTPS/HSTS en OAuth 2.0.
Bij vragen altijd bereid tot toelichting.

Met vriendelijke groet,
Peter Leijnse
Lead architect I&S

Vragen over hoofdstuk 1 "Doelstelling expertadvies"

1. Zijn er volgens u in deze toelichting aanvullingen of anderszins wijzigingen nodig in paragraaf 1.2 en 1.3 ('Aanleiding onderzoek HTTPS en HSTS' en 'Aanpak') bezien vanuit het doel van het document (het Forum en Nationaal Beraad Digitale Overheid voorzien van een inhoudelijk relevante toelichting)?
   Aanleiding en aanpak zijn bekend en duidelijk.

Vragen over hoofdstuk 2 "Toelichting op de standaarden"

2. Zijn er volgens u in deze toelichting aanvullingen of anderszins wijzigingen nodig in hoofdstuk 2 ('Toelichting op de standaarden) bezien vanuit het doel van het document (het Forum en Nationaal Beraad Digitale Overheid voorzien van een inhoudelijk relevante toelichting?
   De beschrijving spitst zich toe op het gebruik van de standaarden binnen 'websites' en 'browsers'. Wij wijzen erop dat het begrip 'webservices' ook van toepassing is op system-to-system-interactie. Bij de authenticatie en beveiliging van dergelijke webservices spelen deels andere overwegingen een rol, waardoor mogelijk ook andere afwegingen worden gemaakt t.a.v. inzet van de beschreven standaarden.

   De beschrijving van HTTPs en TLS illustreert het gebruik van 'server side'-TLS, waarbij de webservice zich bekend maakt bij de client, maar de client onbekend blijft.
   Daarnaast kan ook gebruik gemaakt worden van 'two sided'-TLS, waarbij zowel client als server zich wederzijds bekendmaken. De voorgestelde uitbreiding met HSTS lijkt vooral relevant voor de eerste variant.

   Voor het betrouwbaar en veilig uitwisselen van persoonlijke en vertrouwelijke informatie is het onvoldoende om alleen de server te identificeren. Aanvullend op het gebruik van server-side TLS is daarom ook een adequaat authenticatiemechanisme voor de client noodzakelijk.

Vragen over hoofdstuk 3 "Toetsing van HTTPS aan de criteria"

3. Bent u het eens met de constateringen en conclusies inzake de toegevoegde waarde? [paragraaf 3.1 van het expertadvies]? **Ja.**

4. Bent u het eens met de constateringen en conclusies inzake het open standaardisatieproces? [paragraaf 3.2 van het expertadvies]? **Ja.**

5. Bent u het eens met de constateringen en conclusies inzake het draagvlak? [paragraaf 3.3 van het expertadvies]? **Ja.**

6. Bent u het eens met de constateringen en conclusies inzake de bevordering van de adoptie door opname op de lijst? [paragraaf 3.4 van het expertadvies]? **Ja, met een kleine kanttekening. Adoptie van standaarden die met beveiliging te maken hebben zou niet uitsluitend via het pas-toe-leg-uit-proces, maar vooral vanuit het oogpunt van adequate toepassing van beveiligingsmaatregelen moeten worden gedreven. Het opvolgen van adviezen van het NCSC hoort een directe plaats te hebben in het beveiligingsproces van elke organisatie.**

Vragen over het advies aan het Forum

7. Bent u het eens met de beredenering en conclusie inzake de noodzaak voor de verplichting van HTTPS en HSTS? [paragraaf 4.1 van het expertadvies]
   De consultatie betreft een wijziging t.o.v. de huidige lijsten ('pas-toe-of-let-uit' en 'aanbevolen'). Uit de tekst blijkt niet duidelijk of HTTPs en HSTS als afzonderlijke aanbevolen standaarden worden opgenomen, of in samenhang. Dat laatste lijkt de bedoeling. Dan zou het advies dus luiden: Vervang HTTPs en HSTS op de 'aanbevolen' lijst door 'HTTPs in combinatie met HSTS en NCSC-advies' op de 'pas-toe-of-leg-uit'-lijst.

   De status van HTTP als 'aanbevolen' kan ons inziens behouden blijven, om dezelfde reden dat TLS wordt behouden: ook buiten het toepassings- en werkingsgebied is en blijft dit een aanbevolen standaard. Overigens een die zo alomtegenwoordig is dat opname op welke lijst dan ook enigszins triviaal is.

   HTTPs wordt ook in andere standaarden toegepast, zoals Digikoppeling. HSTS als zodanig wordt daarin nog niet meegenomen. Gezien de toepassing van 'two-sided' TLS binnen Digikoppeling en de verdere mogelijkheden om de client dan wel de organisatie erachter te authenticeren lijkt dit ook niet nuttig.

8. Bent u het eens met het geadviseerde functioneel toepassingsgebied en organisatorisch werkingsgebied? [paragraaf 4.2 van het expertadvies]
   Ja, mits onder 'clients (zoals webbrowsers)' inderdaad alleen webbrowsers worden begrepen, en niet client-server-interactie in system-to-systemverkeer. Voor de laatste categorie prevaleren de afspraken zoals die (binnen het werkingsgebied) binnen Digikoppeling zijn overeengekomen.

9. Bent u het eens met de adoptie-aanbevelingen aan het Nationaal Beraad Digitale Overheid? [paragraaf 4.3 van het expertadvies]
   Ja. Zie overigens vraag 10 voor een aanvullende adoptie-aanbeveling, en vraag 6 voor een alternatieve wijze om adoptie te bevorderen.

Resterende inhoudelijke opmerkingen

10. Is/zijn er volgens u nog andere informatie of overwegingen die aan het Forum en Nationaal Beraad Digitale Overheid zou moeten worden meegegeven voor een besluit over het opnemen van deze standaard op de 'pas toe of leg uit'-lijst?
    Standaarden op de lijst worden doorgaans niet afzonderlijk gebruikt, maar in combinatie. De voorliggende consultatie bevat twee standaarden die te maken hebben met de wijze waarop websites beveiligd kunnen worden. OAuth om de client te authenticeren, TLS om de server te identificeren. Veilige en betrouwbare uitwisseling van vertrouwelijke of persoonlijke informatie heeft beide nodig. 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.

    Dit is vergelijkbaar met de benadering die bij Digikoppeling is toegepast. Daarbij worden communicatie-, beveiligings- en technische aspecten op verschillende niveaus, voor meerdere standaarden in samenhang beschreven. Hiermee wordt voorkomen dat afzonderlijk verplichte standaarden niet in samenhang toepasbaar zijn.

3. Reactie CIBO

Van: Kloosterman, John-Paul
Verzonden: dinsdag 21 maart 2017 12:00
Aan: Forum standaardisatie
Onderwerp: Consultatie Https/hstst, ETSI, OAuth2.0

Geachte lezer,

Vanuit de provincies stuur ik u bij deze de antwoorden op consultatie HTTPS/HSTS, ETSI, OAuth 2.0. Mijn algemene opmerking is dat ik het op prijs zou stellen als er meer met bronverwijzingen gewerkt zou worden. Het kost veel tijd om de expert meningen te toetsen en door bronverwijzingen te gebruiken, worden de adviezen ook veel sterker.

Let daarnaast ook op de consequenties die een standaard op de pas-toe-of-leg-uit-lijst zetten bij de lagere overheden kan hebben. Neem die dan ook mee in de expertgroep -> KING/IBD.

Met vriendelijke groet, John-Paul Kloosterman

Vragen over hoofdstuk 1 "Doelstelling expertadvies"

1. Zijn er volgens u in deze toelichting aanvullingen of anderszins wijzigingen nodig in paragraaf 1.2 en 1.3 ('Aanleiding onderzoek HTTPS en HSTS' en 'Aanpak') bezien vanuit het doel van het document (het Forum en Nationaal Beraad Digitale Overheid voorzien van een inhoudelijk relevante toelichting)? **Antwoord: Nee**

Vragen over hoofdstuk 2 "Toelichting op de standaarden"

2. Zijn er volgens u in deze toelichting aanvullingen of anderszins wijzigingen nodig in paragraaf 1.2 en 1.3 ('Aanleiding onderzoek HTTPS en HSTS' en 'Aanpak') bezien vanuit het doel van het document (het Forum en Nationaal Beraad Digitale Overheid voorzien van een inhoudelijk relevante toelichting)? **Antwoord: Ja, er is meer nodig. Het voorbeeld is namelijk niet volledig. Er wordt onterecht uitgegaan dat het gebruikte certificaat ook bij het domein hoort, maar gaat voorbij de mogelijkheid dat er een certificaat voor een zeer goed lijkend domeinnaam kan worden aangevraagd. Voorstel is om hier te spreken van een Extended certificaat (verplicht) en zelfs een PKI Extended Overheidscertificaat zou nog veel beter zijn.**

   Ander voorstel is om minimale eisen hier vast te stellen. Minimaal TLS 1.2, SHA256 2048 bits sleutellengte.

Vragen over hoofdstuk 3 "Toetsing van HTTPS aan de criteria"

3. Zijn er volgens u in deze toelichting aanvullingen of anderszins wijzigingen nodig in hoofdstuk 2 ('Toelichting op de standaarden) bezien vanuit het doel van het document (het Forum en Nationaal Beraad Digitale Overheid voorzien van een inhoudelijk relevante toelichting? **Antwoord: Ja, mits de aanvullingen toegevoegd worden.**

4. Bent u het eens met de constateringen en conclusies inzake het open standaardisatieproces? [paragraaf 3.2 van het expertadvies]? **Antwoord: Ja.**

5. Bent u het eens met de constateringen en conclusies inzake het draagvlak? [paragraaf 3.3 van het expertadvies]? **Antwoord: Ja, mits de eerder genoemde aanvullingen worden toegevoegd.**

6. Bent u het eens met de constateringen en conclusies inzake de bevordering van de adoptie door opname op de lijst? [paragraaf 3.4 van het expertadvies]? **Antwoord: Ja.**

Vragen over het advies aan het Forum

7. Bent u het eens met de beredenering en conclusie inzake de noodzaak voor de verplichting van HTTPS en HSTS? [paragraaf 4.1 van het expertadvies]
Antwoord: De verwijzing naar de Amerikaanse overheid is niet sterk. Ga uit van de richtlijnen van bijvoorbeeld het NCSC en de richtsnoeren van het AP. De laatste vereist passende beveiligingsmaatregelen en dit zijn er twee van, mits de eerdere punten meegenomen worden. Maak Extended SSL (ja zo wordt het helaas nog genoemd) certificaat hierbij ook verplicht.

Juist de Extended certificaten maken het voor burgers en bedrijven nog veel betrouwbaarder. Pak deze kans om iedereen de juiste kant op te leiden.

8. Bent u het eens met het geadviseerde functioneel toepassingsgebied en organisatorisch werkingsgebied? [paragraaf 4.2 van het expertadvies]
Antwoord: Nee, het is niet volledig. Neem ook mee dat het de bezoeker garanties biedt om daadwerkelijk met een overheidssite van doen te hebben, door naast HTTSP/HSTS ook Extended certificaten te gebruiken. Dus naast een beveiligde verbinding, ook integriteit/autoriteit te kunnen controleren.

9. Bent u het eens met de adoptie-aanbevelingen aan het Nationaal Beraad Digitale Overheid? [paragraaf 4.3 van het expertadvies]
Antwoord: Nee. Punt 1 is veel te lang in de toekomst. De digitale overheid zou dit jaar (2017) toch al rond moeten zijn en het installeren en configureren van een certificaat en HSTS is niet moeilijk. Dit is in een dag te doen en de totale doorlooptijd is een week als er voor een extended certificaat gekozen wordt. Meteen actief maken, doch uiterlijk 1 juli 2017.
Verder akkoord.

Resterende inhoudelijke opmerkingen

10. Is/zijn er volgens u nog andere informatie of overwegingen die aan het Forum en Nationaal Beraad Digitale Overheid zou moeten worden meegegeven voor een besluit over het opnemen van deze standaard op de 'pas toe of leg uit'-lijst?
Antwoord: Ja voeg de eerder genoemde zaken toe. De vrijblijvendheid om voor een onveiligere implementatie te kiezen moet worden tegengegaan.

4. Reactie DICTU

Van: Friso van der Kreeft
Verzonden: vrijdag 3 maart 2017 18:25
Aan: Forum standaardisatie
Onderwerp: Consultatieprocedure HTTPS en HSTS - RE: Openbare consultatie over standaarden voor websitebeveiliging, API-autorisatie en elektronische handtekeningen

Beste collega,

Zie mijn commentaar in de bijlage: Consultatiedocument HTTPS en HSTS –rev.doc

Met vriendelijke groet,

Friso van der Kreeft
Enterprise Architect Informatiebeveiliging

Vragen over hoofdstuk 1 "Doelstelling expertadvies"

2. Zijn er volgens u in deze toelichting aanvullingen of anderszins wijzigingen nodig in paragraaf 1.2 en 1.3 ('Aanleiding onderzoek HTTPS en HSTS' en 'Aanpak') bezien vanuit het doel van het document (het Forum en Nationaal Beraad Digitale Overheid voorzien van een inhoudelijk relevante toelichting)?
   > Nee

Vragen over hoofdstuk 2 "Toelichting op de standaarden"

2. Zijn er volgens u in deze toelichting aanvullingen of anderszins wijzigingen nodig in hoofdstuk 2 ('Toelichting op de standaarden) bezien vanuit het doel van het document (het Forum en Nationaal Beraad Digitale Overheid voorzien van een inhoudelijk relevante toelichting?
   > Suggestie om bij 2.2 deze zin: "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."
   ter volledigheid aan te vullen met een zin zoals: "HSTS biedt dus beveiliging ná het eerste bezoek vanaf de betreffende browser. Die beveiliging werkt zolang de persoon terugkeert binnen de gestelde HSTS verloop tijd. Deze termijn kan van minuten tot oneindig ingesteld worden."

Vragen over hoofdstuk 3 "Toetsing van HTTPS aan de criteria"

3. Bent u het eens met de constateringen en conclusies inzake de toegevoegde waarde? [paragraaf 3.1 van het expertadvies]? **> Ja**

4. Bent u het eens met de constateringen en conclusies inzake het open standaardisatieproces? [paragraaf 3.2 van het expertadvies]? **> Ja**

5. Bent u het eens met de constateringen en conclusies inzake het draagvlak? [paragraaf 3.3 van het expertadvies]? **> Ja**

6. Bent u het eens met de constateringen en conclusies inzake de bevordering van de adoptie door opname op de lijst? [paragraaf 3.4 van het expertadvies]? **> Ja**

Vragen over het advies aan het Forum

7. Bent u het eens met de beredenering en conclusie inzake de noodzaak voor de verplichting van HTTPS en HSTS? [paragraaf 4.1 van het expertadvies] **> Ja**

8. Bent u het eens met het geadviseerde functioneel toepassingsgebied en organisatorisch werkingsgebied? [paragraaf 4.2 van het expertadvies] **> Ja**

9. Bent u het eens met de adoptie-aanbevelingen aan het Nationaal Beraad Digitale Overheid? [paragraaf 4.3 van het expertadvies] **> Ja**

Resterende inhoudelijke opmerkingen

10. Is/zijn er volgens u nog andere informatie of overwegingen die aan het Forum en Nationaal Beraad Digitale Overheid zou moeten worden meegegeven voor een besluit over het opnemen van deze standaard op de 'pas toe of leg uit'-lijst? **> Ja: De vertrouwelijkheid en intergiteit wordt verhoogd m.b.v. HSTS. Prima. Vertrouwen wordt technisch opgebouwd in de volgorde: DNSSEC > HSTS > https > PKIoverheid > enz.**

    Wat ik nog mis is het begin van vertrouwen. Waarom zou iemand belastingdienst.nl wel vertrouwen en aangifte-belastingdienst.nl niet?

    Rijksbreed is afgesproken:
    De Dienst Publiek en Communicatie (DPC) is registrar en houder van alle domeinnamen van de Rijksoverheid. Indien van toepassing moeten deze worden geregistreerd in het Webregister Rijksoverheid.

    Domeinnaambeleid en PKIoverheid afspraken:
    https://www.communicatierijk.nl/vakkennis/r/rijkswebsites-verplichte-richtlijnen/. Dan kan iemand mbv www.sidn.nl zien dat de website door MinAZ geregistreerd is en DUS een echte overheidswebsite is.

    Het Webregister Rijksoverheid wordt onderhouden door MinAZ:
    https://www.communicatierijk.nl/vakkennis/r/rijkswebsites-verplichte-richtlijnen/inhoud/websiteregister
    Dan kan iemand mbv dit webregister (document) zien dat de website DUS een echte overheidswebsite is.

    Wellicht is het een idee om niet alleen Rijksbreed, maar overheidsbreed bovenstaande af te spreken?

Datum
28 maart 2017

5. Reactie Bas Meijer

Van: Bas Meijer
Verzonden: donderdag 2 maart 2017 10:04
Aan: Forum standaardisatie
Onderwerp: Consultatie NCSC-NL inzake HTTPS en HSTS

Beste Beste,

Bijlage "Consultatiedocument HTTPS en HSTS.docx" is mijn reactie op uw expertadvies.

met vriendelijke groeten,

Bas Meijer

Vragen over hoofdstuk 1 "Doelstelling expertadvies"

1. Zijn er volgens u in deze toelichting aanvullingen of anderszins wijzigingen nodig in paragraaf 1.2 en 1.3 ('Aanleiding onderzoek HTTPS en HSTS' en 'Aanpak') bezien vanuit het doel van het document (het Forum en Nationaal Beraad Digitale Overheid voorzien van een inhoudelijk relevante toelichting)?
   HTTPS (RFC 2818), HSTS (RFC 6797), HPKP (RFC 7469) en TLS zijn opgenomen op de lijst met open standaarden.

   Verder steeds "HTTPS en HSTS" vervangen door: "HTTPS, HSTS en HPKP" HPKP is niet opgenomen.

Vragen over hoofdstuk 2 "Toelichting op de standaarden"

2. Zijn er volgens u in deze toelichting aanvullingen of anderszins wijzigingen nodig in paragraaf 1.2 en 1.3 ('Aanleiding onderzoek HTTPS en HSTS' en 'Aanpak') bezien vanuit het doel van het document (het Forum en Nationaal Beraad Digitale Overheid voorzien van een inhoudelijk relevante toelichting)?
   ... "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." In de praktijk wordt bij bedrijven vaak een proxy met "ssl-inspection" gecombineerd met "policy-push" van een bedrijfseigen CA certificaat. Misbruik door systeembeheerders is daardoor eenvoudig. Er hoeft geen algoritme gekraakt te worden. HPKP beschermt tegen dit misbruik omdat een site kan aangeven welke autoriteit bevoegd is om haar certificaat te verstrekken.

   ... "HTTPS beschermt de data zodat het niet gewijzigd of overruled kan worden" zolang de "trusted certificate store" inderdaad vertrouwde derde partijen bevat. De leveranciers van Windows en OSX werken samen met allerlei partijen die niet noodzakelijkerwijs vertrouwd worden door de eindgebruiker. De eindgebruiker vertrouwd niet noodzakelijkerwijs de systeembeheerder.

Vragen over hoofdstuk 3 "Toetsing van HTTPS aan de criteria"

3. Zijn er volgens u in deze toelichting aanvullingen of anderszins wijzigingen nodig in hoofdstuk 2 ('Toelichting op de standaarden) bezien vanuit het doel van het document (het Forum en Nationaal Beraad Digitale Overheid voorzien van een inhoudelijk relevante toelichting?
   geen commentaar
4. Bent u het eens met de constateringen en conclusies inzake het open standaardisatieproces? [paragraaf 3.2 van het expertadvies]?
   Aanvullend: HTTPS is belangrijk, maar complex, en het is niet de enige methode om websites te beveiligen. Bovendien is deze wereld voortdurend in verandering, IETF formaliseert open standaarden, maar praktisch gezien zijn er gelukkig websites die snel kunnen helpen bij het toetsen van HTTPS/TLS, ook aan andere (internationale) normen: PCI, NIST, HIPAA. https://observatory.mozilla.org is een goed startpunt.

5. Bent u het eens met de constateringen en conclusies inzake het draagvlak? [paragraaf 3.3 van het expertadvies]? **Geen commentaar**

6. Bent u het eens met de constateringen en conclusies inzake de bevordering van de adoptie door opname op de lijst? [paragraaf 3.4 van het expertadvies]? **Met toevoeging van HPKP.**

<u>Vragen over het advies aan het Forum</u>

7. Bent u het eens met de beredenering en conclusie inzake de noodzaak voor de verplichting van HTTPS en HSTS? [paragraaf 4.1 van het expertadvies] **Nee, het risico in bovengenoemd scenario van de proxybeheerder als "man in the middle" waarborgt vertrouwelijkheid onvoldoende.**

8. Bent u het eens met het geadviseerde functioneel toepassingsgebied en organisatorisch werkingsgebied? [paragraaf 4.2 van het expertadvies] **Nee, de intranetten en client-pc's van de overheid moeten nagekeken worden op root-certificaten die niet vertrouwd zijn. Deze moeten worden verwijderd.**

9. Bent u het eens met de adoptie-aanbevelingen aan het Nationaal Beraad Digitale Overheid? [paragraaf 4.3 van het expertadvies] **Geen commentaar.**

<u>Resterende inhoudelijke opmerkingen</u>

10. Is/zijn er volgens u nog andere informatie of overwegingen die aan het Forum en Nationaal Beraad Digitale Overheid zou moeten worden meegegeven voor een besluit over het opnemen van deze standaard op de 'pas toe of leg uit'-lijst? **Overweeg een digitaal certificaat (S/MIME) naast het paspoort.**