FS-20140415.04C

Forum Standaardisatie

Wilhelmina v Pruisenweg 104
2595 AN Den Haag
Postbus 84011
2508 AA Den Haag
www.forumstandaardisatie.nl

notitie

Opname DANE op de lijst voor 'pas-toe-of-leg-uit'

FORUM STANDAARDISATIE

Agendapunt:	Open standaarden, lijsten		
Bijlagen:	1. Expertadvies 2. Overzicht reacties consultatieronde		
Aan:	Forum Standaardisatie		
Van:	Stuurgroep Standaardisatie		
Datum:	03-04-2014	**Versie**	1.0
Betreft:	Opname DANE op de lijst voor 'pas toe of leg uit'		

Waarom is een keuze belangrijk?
Servercertificaten moeten de bezoeker van overheidswebsites het vertrouwen bieden dat ze ook daadwerkelijk deze overheidssite bezoeken en niet een vervalste site. Nu wordt een internetverbinding meestal beveiligd door verificatie van deze (gepubliceerde) certificaten bij een Certificaat Service Provider. Met DANE heeft een overheidsorganisatie als domeinhouder de mogelijkheid om in aanvulling op de PKI-infrastructuur zelf een extra verificatiemogelijkheid te bieden, namelijk via het Domain Name System (DNS) van het internet. Dit biedt twee onafhankelijke verificatiemethoden die in combinatie moeilijker te kraken zijn dan het huidige systeem.

Hoe is het advies tot stand gekomen?
Op basis van een intakegesprek met de aanmelder is geadviseerd om DANE (tegelijkertijd met TLS 1.2) in procedure te nemen. Op 23 januari 2014 is een expertgroep met vertegenwoordigers uit het bedrijfsleven en de overheid bijeengekomen. De expertgroep heeft geadviseerd om de standaard niet op te nemen op de lijst van 'pas toe of leg uit'. Het expertadvies is gepubliceerd ten behoeve van een openbare consultatie, die heeft geleid tot reacties van KING en het ministerie van Binnenlandse Zaken en Koninkrijksrelaties (hierna ministerie van BZK). Deze reacties hebben niet geleid tot een ander advies dan het expertadvies.

Zijn er risico's verbonden aan de keuze?
DANE voegt een extra check toe aan het huidige PKI(overheid)-systeem, waardoor overheidswebsites voor hun vertrouwelijkheid minder afhankelijk zijn van extern beheerde en uitgegeven certificaten. Dat helpt zo veiligheidsrisico's te verkleinen. De Diginotar-affaire heeft ons geleerd dat verlaging van de veiligheidsrisico's wenselijk is. DANE is echter nog niet breed in gebruik en eventuele problemen met dit nieuwe beveiligingsprotocol moeten nog aan het licht komen.

Gevraagd besluit

Datum
4 april 2014

Het Forum Standaardisatie wordt gevraagd in te stemmen met:
1. Het advies om DANE niet op te nemen op de lijst voor 'pas toe of leg uit'.
2. De additionele adviezen ten aanzien van de adoptie van de standaard.

Ad 1) Het advies DANE niet op te nemen op de lijst voor 'pas toe of leg uit'
De expertgroep schat in dat:
- De huidige marktondersteuning voor de toepassing van DANE onvoldoende is.
- De toepassing van de standaard binnen de publieke sector en andere sectoren onvoldoende is. Er is nog te weinig praktijkervaring om te toetsen wat de impact en het effect van de standaard is.

Geadviseerd wordt dan ook om de standaard DANE nog niet op te nemen op de lijst van 'pas toe of leg uit'.

Ad 2) Additionele adviezen ten aanzien van de adoptie van de standaard
Ten aanzien van de adoptie van de standaard worden de volgende additionele adviezen gedaan:
1. Forum Standaardisatie wordt opgeroepen om, als onderdeel van het dossier Samenhang, DANE mee te nemen in de schets en beschrijving van de samenhang tussen de beveiligingsstandaarden op de lijsten.
2. Indiener stichting NLnet en de expertgroep in brede zin worden opgeroepen om het Forum op de hoogte te houden van ontwikkelingen rond de standaard. Op het moment dat er sprake is van een meer grootschalige toepassing van DANE, kunnen de bevindingen van deze expertgroep nogmaals tegen het licht worden gehouden.

Toelichting

Waar gaat het inhoudelijk over?
Servercertificaten moeten de bezoeker van overheidswebsites het vertrouwen bieden dat ze ook daadwerkelijk deze overheidssite bezoeken en niet een vervalste site. Nu wordt een internetverbinding meestal beveiligd door verificatie van deze (gepubliceerde) certificaten bij een Certificaat Service Provider. DANE is een standaard die het mogelijk maakt om certificaten voor het beveiligen van internetverbindingen op een alternatieve manier te publiceren en te verifiëren, namelijk via het Domain Name System (DNS) van het internet.

DANE is daarbij een uitbreiding op de DNSSEC-standaard, die al op de 'pas toe of leg uit'-lijst staat. Door het invoegen van (een afschrift van) een certificaat in het DNS (het zogenaamde TLSA-record) en deze cryptografisch te beveiligen met DNSSEC, kan het servercertificaat dat een (overheids)website aanbiedt, via het DNS worden geverifieerd. DANE biedt de optie om dit naast de bestaande verificatie via een Certificaat Service Provider te doen.

DANE zorgt voor een aanvulling op de gecentraliseerde PKI(overheid) infrastructuur, waarbij overheden als domeinnaamhouders voor hun servercertificaten niet meer uitsluitend afhankelijk zijn van echtheidsgaranties door certificaatautoriteiten. In principe biedt dit twee onafhankelijke verificatiemethoden die in combinatie moeilijker te kraken zijn dan het huidige systeem. Voorwaarden

hiervoor zijn een goede configuratie en procesmatige uitvoer volgens de juiste beveiligingsvoorschriften.

Hoe is het proces verlopen?
Op basis van een intakegesprek met de aanmelder is geadviseerd om DANE in procedure te nemen, om de samenhang met andere internet beveiligingsstandaarden te onderzoeken en om het gebruik en het draagvlak bij overheden in Nederland te onderzoeken. Op 23 januari 2014 is een expertgroep met vertegenwoordigers uit het bedrijfsleven en de overheid bijeengekomen. De expertgroep heeft geadviseerd om de standaard nog niet op te nemen op de lijst van 'pas toe of leg uit'. Het expertadvies is gepubliceerd ten behoeve van een openbare consultatie, die heeft geleid tot reacties van KING en BZK. Deze reacties hebben niet tot een ander advies dan het expertadvies geleid.

Wat is het toepassings- en werkingsgebied
Als toepassingsgebied wordt voorgesteld:
"Het publiceren en verifiëren van certificaten ter beveiliging van internetverbindingen bij gebruik van DNSSEC".

En als werkingsgebied:
"Overheden (Rijk, provincies, gemeenten en waterschappen) en instellingen uit de (semi)publieke sector."

Hoe scoort de standaard op de toetsingscriteria?

<u>Open standaardisatieproces</u>
De standaard wordt beheerd door IETF. Deze organisatie heeft goed gedocumenteerde en open beheerprocedures. Er is geen lidmaatschap, iedereen kan wijzigingsverzoeken indienen, en het beheerproces en de besluitvorming zijn open en transparant. Er zijn geen kosten verbonden aan het downloaden van de specificatie en het implementeren van de standaard.

<u>Toegevoegde waarde</u>
De toegevoegde waarde van DANE is dat het enkele beveiligingsrisico's adresseert. Nu zijn overheidswebsites voor hun vertrouwelijkheid afhankelijk van extern beheerde en uitgegeven certificaten. Met DANE heeft een overheidsorganisatie als domeinhouder de mogelijkheid om, in aanvulling op de PKI-infrastructuur, zelf een extra verificatiemogelijkheid te bieden via DNS. Dit biedt twee onafhankelijke verificatiemethoden die in combinatie moeilijker te kraken zijn dan het huidige systeem.

<u>Draagvlak</u>
Levering van commerciële producten voor de DANE-standaard is mogelijk, maar er zijn nauwelijks complete, off-the-shelf producten beschikbaar. Dit geldt zowel voor producten op client systemen (browsers) als voor tools die operationele processen aan de serverzijde ondersteunen (b.v. management van encryptiesleutels). Mondiaal zijn er nog geen grootschalige toepassingen van DANE bekend. De beschikbare operationele ervaring is dan ook zeer beperkt en binnen de Nederlandse publieke sector is voor zover bekend nog geen ervaring met het gebruik van de standaard.

Opname bevordert de adoptie
De expertgroep is van mening dat het opnemen van DANE op de 'pas toe of leg uit'-lijst op dit moment niet het gewenste middel is om adoptie te bevorderen. De meerderheid van de expertgroep geeft aan dat (a) de huidige marktondersteuning beperkt is en (b) de toepassing van en ervaring met de standaard door andere partijen momenteel onvoldoende is.

Wat is de conclusie van de expertgroep en de consultatie?

Conclusie van de expertgroep
De expertgroep adviseert de standaard DANE nog niet op te nemen op de lijst van 'pas toe of leg uit'.

Toelichting van eventuele risico's
Er zijn tijdens de toetsing en consultatie geen specifieke risico's aan het nog niet opnemen van de standaard naar voren gekomen.

Eventuele aanvullingen vanuit de consultatie
In de consultatieronde zijn door het ministerie van Binnenlandse Zaken (OBR ICCIO) bedenkingen geplaatst bij de opname van operationele beveiligingsstandaarden (zoals DANE) op de lijst voor 'pas toe of leg uit'. De 'pas toe of leg uit'-lijst is er in hun zienswijze voor om de adoptie van open standaarden te bevorderen als er momenteel gebruik gemaakt wordt van gesloten standaarden. Dat is bij DANE niet het geval, hier speelt voornamelijk informatiebeveiliging een rol. Verder is het de verantwoordelijkheid van het (lijn)management om risico's te inventariseren en de keuze te maken welke maatregelen worden genomen.

Reactie
In het instellingsbesluit is echter opgenomen dat de taak van het College en Forum Standaardisatie onder andere betrekking heeft op "veilige en betrouwbare uitwisseling en (her)gebruik van gegevens". Ook staat het thema informatiebeveiliging al twee jaar in het werkplan van het Forum en geven organisaties als het NCSC aan dat de lijst wordt gezien als extra drukmiddel voor veilige gegevensuitwisseling. Operationele beveiligingsstandaarden zouden dan ook op de 'pas toe of leg uit'-lijst kunnen worden geplaatst, wat in het verleden ook vaak is voorgekomen.

KING (IBD) onderschrijft het expertadvies om DANE nog niet op te nemen op de 'pas toe of leg uit'-lijst en geeft aan nu dan ook niets met DANE te doen.

Welke additionele adviezen zijn er ten aanzien van de adoptie van de standaard?
Ten aanzien van de adoptie van de standaard worden de volgende additionele adviezen gedaan:

1. Forum Standaardisatie wordt opgeroepen om, als onderdeel van het dossier Samenhang, DANE mee te nemen in de schets en beschrijving van de samenhang tussen de beveiligingsstandaarden op de lijsten.

2. Indiener Stichting NLnet en de expertgroep in brede zin worden opgeroepen om het Forum op de hoogte te houden van ontwikkelingen rond de standaard. Op het moment dat er sprake is van meer grootschalige toepassing van DANE, kunnen de bevindingen van deze expertgroep nogmaals tegen het licht worden gehouden.

Bijlage

Datum
4 april 2014

- Expertadvies DANE, zie: (https://lijsten.forumstandaardisatie.nl/open-standaard/dane)
- Overzicht reacties consultatieronde, zie: (https://lijsten.forumstandaardisatie.nl/open-standaard/dane)