notitie

Aan: Forum Standaardisatie

Van: Bureau Forum Standaardisatie

Datum: 11 september 2018

Versie: 1.0

Betreft: Reacties uit de openbare consultatie S/MIME (aanbeveling voor alleen digitaal ondertekenen van e-mail)

Inleiding

Dit document bevat de reacties die tussen 6 augustus en 10 september werden ontvangen op de openbare consultatie voor het plaatsen van S/MIME op de lijst aanbevolen standaarden van het Forum Standaardisatie, alleen voor digitale ondertekening (en niet voor versleuteling) van e-mail. In totaal is een vijftal reacties ontvangen van RINIS, het Ministerie van Defensie, de Sociale Verzekeringsbank (SVB), het Uitvoeringsinstituut Werknemersverzekeringen (UWV) en de Kamer van Koophandel (KvK).

De reacties, die als e-mail binnenkwamen, zijn in zijn originele vorm zonder bewerking weergegeven in chronologische volgorde van binnenkomst. Wel zijn de contactgegevens en is voor deze consultatie niet-relevante tekstverwijderd.

Reacties uit de openbare consultatie

Reactie van RINIS

Van: Rob Verweij <…>
Verzonden: maandag 20 augustus 2018 09:16
Aan: Zuidweg, J. (Han) - Forum Standaardisatie <han.zuidweg@forumstandaardisatie.nl>
Onderwerp: Re: Openbare consultatie

Dag Han,

… *[niet voor deze openbare consultatie relevante tekst verwijderd]*

Van onze (architect) kant de volgende reactie op de gedane adviezen:

… *[niet voor deze openbare consultatie relevante tekst verwijderd]*

S/MIME niet meer gebruiken voor encryptie, denk dat het goed is om het advies van het NCSC hier te volgen en dus eens. Alleen is het wel goed om de S/MIME standaard goed in de gaten te houden want er komt een nieuwe versie waarin maatregelen zijn opgenomen tegen de door EFAIL geconstateerde problemen.

Met vriendelijke groet,
Rob Verweij
directeur
RINIS

Reactie van het Ministerie van Defensie

[Deze reactie van het Ministerie van Defensie ontvingen wij per e-mail als nota in PDF formaat met referentie BS2018021556. Onderstaande tekst is integraal overgenomen uit deze nota.]

Deze reactie is opgesteld naar aanleiding van de openbare consultatie over S/MIME voor digitale ondertekening door het Forum Standaardisatie. De antwoorden zijn genummerd met dezelfde nummers als de vragen in het Consultatiedocument S/MIME voor digitale ondertekening.

Toelichting gebruikte begrippen

Deze reactie gebruikt de termen 'vertrouwelijk' en 'integer' houden van e-mail uitwisseling. Zie de VIR2007 voor de definities van vertrouwelijkheid en integriteit. Versleuteling is een methode om de vertrouwelijkheid van informatie (hier e-mails) te borgen. Digitale ondertekening is een methode om de integriteit van informatie te borgen. In deze reactie worden de termen 'vertrouwelijk' en 'integer' gebruikt wanneer wordt verwezen naar het gewenste doel. De termen 'versleuteling' en 'digitale ondertekening' worden gebruikt wanneer wordt verwezen naar de methoden waarmee die doelen bereikt kunnen worden.

Antwoorden op de gestelde vragen

1. Nee. Defensie heeft de volgende bezwaren tegen het op de lijst van aanbevolen standaarden plaatsen en daarmee gebruiken van S/MIME voor alleen digitale ondertekening:

1. Een oplossing voor het alleen integer kunnen uitwisselen van email is niet goed genoeg. Voor het veilig uitwisselen van e-mail maakt Defensie altijd afspraken over het vertrouwelijk en integer uitwisselen van e-mail met de betrokken partijen. Defensie zal daarom alleen standaarden ondersteunen die zowel vertrouwelijke als integere uitwisseling van e-mail mogelijk maken. Gezien de gevonden kwetsbaarheid op het vlak van vertrouwelijkheid valt S/MIME af als oplossing.
2. De kans dat gebruikers S/MIME foutief gaan inzetten is te groot. De S/MIME standaard en implementaties geven gebruikers de mogelijkheid e-mail te versleutelen en/of te ondertekenen. Wanneer S/MIME aan gebruikers wordt aangeboden voor het ondertekenen van e-mail is de kans groot dat ze het ook zullen gaan gebruiken voor het versleutelen van e-mail. Veel gebruikers zullen zich niet realiseren dat het versleutelen van e-mail met S/MIME de vertrouwelijkheid van de e-mail niet borgt door de gevonden kwetsbaarheid. Alleen standaarden en implementaties die e-mail vertrouwelijk en integer uitwisselen, behoeden gebruikers voor vergissingen. S/MIME voldoet hier niet aan.
3. S/MIME heeft een lage adoptiegraad bij de partijen waarmee Defensie vertrouwelijk en/of integer e-mail uitwisselt. Er zijn een relatief groot aantal oplossingen voor het vertrouwelijk en/of integer uitwisselen van e-mail. Defensie maakt per partij aparte afspraken hierover. Het merendeel van de partijen bevindt zich buiten de Nederlandse (semi-)overheid. Voorbeelden zijn defensiepartners in NAVO en EU verband, en leveranciers waarmee (soms sector breed) afspraken worden gemaakt. Door de lage adoptiegraad van S/MIME voldoet S/MIME voor digitale ondertekening niet aan het criterium voor een aanbevolen standaard.
4. De baten wegen niet op tegen de lasten. Elke afspraak over het vertrouwelijk en/of integer uitwisselen van e-mail bevat ook afspraken over het type certificaat dat wordt gebruikt en de manier waarop het certificaatbeheer wordt uitgevoerd. Zo ontstaan ook voor de implementatie van S/MIME voor digitale ondertekening aanzienlijke kosten terwijl de baten alleen het integer houden van e-mail uitwisseling betreffen. Bij de alternatieve oplossingen leveren dezelfde kosten hogere baten op; namelijk het zowel vertrouwelijk als integer kunnen uitwisselen van e-mail.

2. Ja.

3. Bij een op dit moment lopende aanbesteding wordt de mogelijkheid voor het versleutelen en/of digitaal ondertekenen benoemt. Gezien de beschikbaarheid van verschillende oplossingen voor versleuteling en/of ondertekening is aan de leveranciers gevraagd zelf oplossingen (mogelijk een oplossing) te kiezen en aan te bieden. Daar waar Defensie geen andere afspraken maakt met partners zal de door de leverancier aangeboden oplossing gebruikt gaan worden. Defensie kan pas aangeven welke oplossing dit is nadat de betreffende aanbesteding is gegund.

Bestuursadviseur Architectuur

Ir. M.J.A. van Adrichem

Reactie van de Sociale Verzekeringsbank

Van: Visser, T.
Verzonden: maandag 10 september 2018 14:11
Aan: Zuidweg, J. (Han) - Forum Standaardisatie <han.zuidweg@forumstandaardisatie.nl>
CC: Oberendorff, L. (Ludwig) - Forum Standaardisatie <ludwig.oberendorff@forumstandaardisatie.nl>
Onderwerp: FW: Openbare consultatie verplichte en aanbevolen standaarden

Beste Han,

Ik begrijp dat UWV zelf een reactie zal sturen. Hierbij de ruwe reactie van SVB.

Met vriendelijke groet,

Teun Visser
.....
Ministerie van Sociale Zaken en Werkgelegenheid
Directoraat-generaal Sociale Zekerheid en Integratie
Directie Stelsel en Volksverzekeringen
Afdeling Handhaving en Gegevensuitwisseling

Van: Verheij, Fransje (Sociale Verzekeringsbank) <…>
Verzonden: dinsdag 28 augustus 2018 18:24
Aan: Visser, T. <..>
CC: …
Onderwerp: RE: Openbare consultatie verplichte en aanbevolen standaarden

Hallo Teun en Ron,

Ik heb de vraag over de consultatie uitgezet bij Geer Haas. Hieronder zijn antwoord:

Hi Fransje,

Mijn samenvatting:

…[*Niet voor deze consultatie relevante tekst verwijderd]*

Aanbevolen standaarden zijn nuttig maar zullen alleen daar toepassen waar expliciet nodig gevraagd. E.e.a. hangt m.n. samen met adoptiegraad.

En de geconsolideerde feedback (als gekregen van onze experts) op de consultatie:

… [Niet voor deze consultatie relevante tekst verwijderd]

Consultatiedocument S/MIME

Vraag 1: Ja, eens

Vraag 2: Ja, eens

Vraag 3: Nee

… [Niet voor deze consultatie relevante tekst verwijderd]

Reactie van het Uitvoeringsinstituut Werknemersverzekeringen

Van: Vierbergen, Kato (K.R.) <…>
Verzonden: dinsdag 11 september 2018 16:22
Aan: Forum standaardisatie <forumstandaardisatie@logius.nl>; Knubben, B.S.J. (Bart) - Forum Standaardisatie <…>
CC: Bos, Ron (R.) <…>; Franken, Leo (L.) <…>
Onderwerp: reactie UWV openbare consultatie Open Standaarden

L.S.,

In reactie op de openbare consultatie Open Standaarden en plaatsing op de PTOLU-lijst stuur ik jullie hierbij de input vanuit UWV.

Het betreft de consultatie: https://www.forumstandaardisatie.nl/thema/openbare-consultatie

… [Niet voor deze consultatie relevante tekst verwijderd]

Het advies om de standaard S/MIME (e-mail beveiliging) alleen voor digitale ondertekening van e-mail (niet voor versleuteling van berichten) op de lijst aanbevolen standaarden te plaatsen. Ja

Als er vragen zijn, hoor ik dat graag.

Met vriendelijke groet,

Kàto Vierbergen-Schuit
Beleidadviseur Security en Privacy / Information Security Officer
UWV ICT

Reactie van de Kamer van Koophandel

[Deze reactie van de Kamer van Koophandel ontvingen wij per e-mail als bijlage in .doc formaat. Hieronder is het commentaar in de bijlage weergegeven in de oorspronkelijke tekst en gerangschikt per vraag.]

Kamer van Koophandel Advies
Datum: 10 september 2018
Auteur: Frits Maas ICT Architect Kamer van Koophandel

Opname van S/MIME op de lijst aanbevolen standaarden, uitsluitend voor digitale ondertekening van e-mail
Consultatiedocument S/MIME voor digitale ondertekening Datum 5 augustus 2018

1. KvK: Ja

2. KvK: Ja

3. KvK:

a. S/Mime maakt gebruik van keys en/of certifictaten. Na het lezen van diverse artikelen zie ik grote problemen bij het plaatsen van deze standaard op de lijst. Microsoft geeft aan dat S/Mime alleen werkt binnen de eigen Exchange omgeving, Apple geeft aan dat je vóór het verzenden van mail het certificaat van de ontvanger nodig hebt. Verder zie ik nogal wat administratieve problemen m.b.t. het verstrekken én bijhouden van certificaten. In het geval van de KvK zou het erop neerkomen dat wij meer dan 2000 certificaten nodig hebben. En wat te doen met certificaten die ingetrokken worden of verlopen? Zijn die mails dan nog leesbaar?
b. Ja zeker in het licht van de recentelijk ontdekte zwakheden. Maar ook de gebrekkige implementatie van de diverse vendoren waardoor er geen zekerheid is over de correcte werking van de versleuteling. Daarnaast met het plaatsen van STARTTLS DANE voor verzendende servers op de PTOLU lijst is noodzaak voor S/MIME versleuteling minder noodzakelijk.