Forum Standaardisatie

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

notitie

Opname S/MIME 3.2 (standaard voor aanvullende beveiliging van e-mail) op de lijst met open standaarden

FORUM STANDAARDISATIE 25 april 2018

Agendapunt:	3G		
Bijlagen:	Expertadvies S/MIME 3.2-standaard en overzicht reacties consultatieronde		
Aan:	Forum Standaardisatie		
Van:	Stuurgroep Open Standaarden		
Datum:	3 april 2018	**Versie**	1.0

Aanleiding en achtergrond

S/MIME 3.2 (standaard voor aanvullende beveiliging van e-mail) beschermt de vertrouwelijkheid en authenticiteit van e-mail uitwisseling tussen een verzendende en ontvangende e-mail client. De e-mail veiligheidstandaarden SPF, DKIM, DMARC, STARTTLS en DANE die al op de 'pas toe of leg uit' lijst staan, verzorgen veilige gegevensuitwisseling tussen e-mailservers. Tussen e-mail client en e-mai server bieden deze standaarden echter geen bescherming. De toegevoegde waarde van S/MIME is dat een derde geen misbruik kan maken van de identiteit van iemand anders, onderschepte e-mails niet kan lezen, en de inhoud van een e-mail niet kan manipuleren zonder dat dit opgemerkt wordt.

De implementatie van S/MIME in e-mailapplicaties zorgt ervoor dat de ontvanger van een met S/MIME vercijferde en getekende e-mail kan zien of een e-mail veilig is. E-mail clients en webmail applicaties die S/MIME ondersteunen laten een grafisch icoon (zegel of slotje) zien wanneer het bericht met S/MIME is ondertekend, naar analogie met het 'hangslotje' in de browser wanneer de verbinding met een website veilig is. Ontvangers zonder technische kennis van S/MIME kunnen zo van de standaard gebruik van maken.

Zonder gebruik van S/MIME kan het voorkomen dat er misbruik wordt gemaakt van de identiteit van personen, dat e-mails gelezen of gemanipuleerd kunnen worden op het pad tussen de verzendende en ontvangende e-mail client. Met gebruik van S/MIME wordt de veiligheid van het e-mailverkeer tussen verzendende en ontvangende applicatie gewaarborgd. Alleen als een derde in bezit komt van de geheime sleutel van een gebruiker kan hier misbruik van gemaakt worden.

S/MIME kan bescherming bieden in een situatie waarin veiligheidsmaatregelen zoals SPF, DKIM, DMARC, STARTTLS en DANE ontbreken of wanneer de integriteit van de mailservers niet vertrouwd kan worden. S/MIME kan zowel in combinatie met SPF, DKIM, DMARC, STARTTLS en DANE als alleenstaand gebruikt worden.

Geadviseerd wordt om S/MIME 3.2 als 'aanbevolen'-standaard op de lijst met open standaarden te nemen.

Betrokkenen en proces
De procesbegeleider heeft op 3 november 2017 een intakegesprek gevoerd met de indiener. Tijdens de intake is de standaard getoetst op criteria voor het in procedure nemen en is een eerste inschatting gemaakt van de kansrijkheid van de procedure. Op basis van de intake heeft het Forum Standaardisatie op 13 december 2017 besloten de aanmelding in procedure te nemen. Hierop volgend zijn experts benaderd. Op basis van de aanmelding en de intake is een concept expertadvies opgesteld voor de experts. De procesbegeleider heeft een concept van dit expertadvies aan de leden van de expertgroep gestuurd met verzoek om commentaar. Na verwerking van reacties is het rapport nogmaals toegestuurd aan de experts, afgerond en ingediend bij het Bureau Forum Standaardisatie (het secretariaat van het Forum Standaardisatie) ten behoeve van de publieke consultatieronde. Het expertadvies is vervolgens van 23 februari – 23 maart 2018 beschikbaar gesteld voor publieke consultatie. VNG, DICTU en SURFnet hebben tijdens de openbare consultatie een reactie gegeven op het expertadvies van S/MIME. Deze reacties wijzen op relevante aspecten van S/MIME maar geven geen aanleiding om het positieve expertadvies te wijzigen.

Consequenties en vervolgstappen
Er zijn geen specifieke risico's verbonden aan de keuze. Het Forum Standaardisatie zal op basis van het Forumadvies een advies aan het Overheidsbreed Beleidsoverleg Digitale Overheid opstellen. Het Overheidsbreed Beleidsoverleg Digitale Overheid bepaalt op basis van het advies of S/MIME 3.2 op de lijst met open standaarden wordt opgenomen met als status 'aanbevolen'.

Gevraagd besluit

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

Het Forum Standaardisatie adviseert het Overheidsbreed Beleidsoverleg Digitale Overheid om:
1. S/MIME 3.2 op te nemen op de lijst met aanbevolen standaarden voor het hieronder geformuleerde toepassings- en organisatorisch werkingsgebied.
2. In te stemmen met de additionele adviezen ten aanzien van de adoptie van S/MIME 3.2, zoals hieronder geformuleerd.

Ad 1
Geadviseerd wordt om S/MIME 3.2 op te nemen op de lijst aanbevolen standaarden.

Als functioneel toepassingsgebied voor S/MIME wordt geadviseerd:
S/MIME kan worden toegepast op mailverkeer wanneer een aanvullende beveiliging nodig is.

Omdat S/MIME is aangemeld voor de lijst aanbevolen standaarden heeft het functioneel toepassingsgebied geen verplichtend karakter.

Als organisatorisch werkingsgebied van S/MIME wordt geadviseerd:

Nederlandse overheden (Rijk, provincies, gemeenten en waterschappen) en instellingen uit de (semi-) publieke sector.

Omdat S/MIME is aangemeld voor de lijst aanbevolen standaarden heeft het organisatorisch werkingsgebied geen verplichtend karakter.

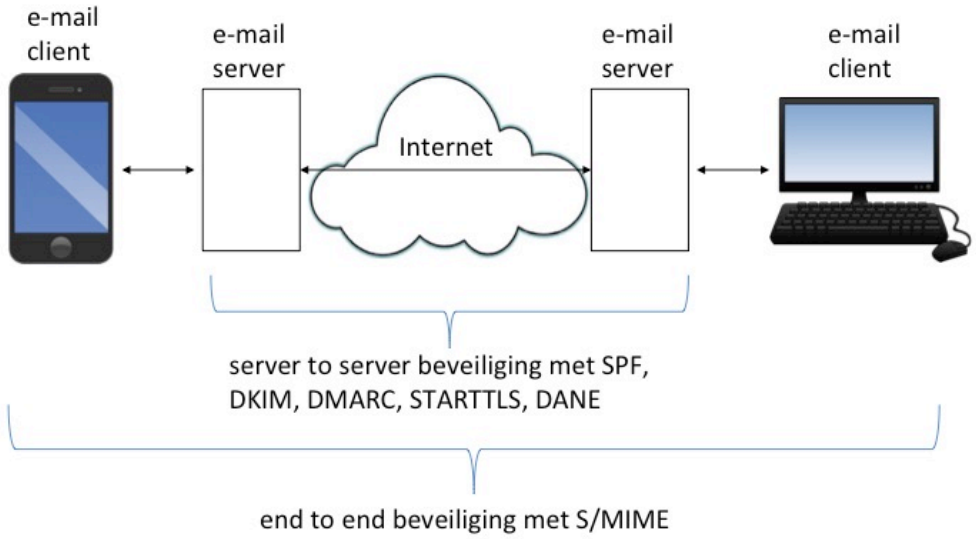
Ad 2 Additionele adviezen ten aanzien van de adoptie van de standaard
Ten aanzien van de adoptie van de standaard worden de volgende oproepen gedaan:

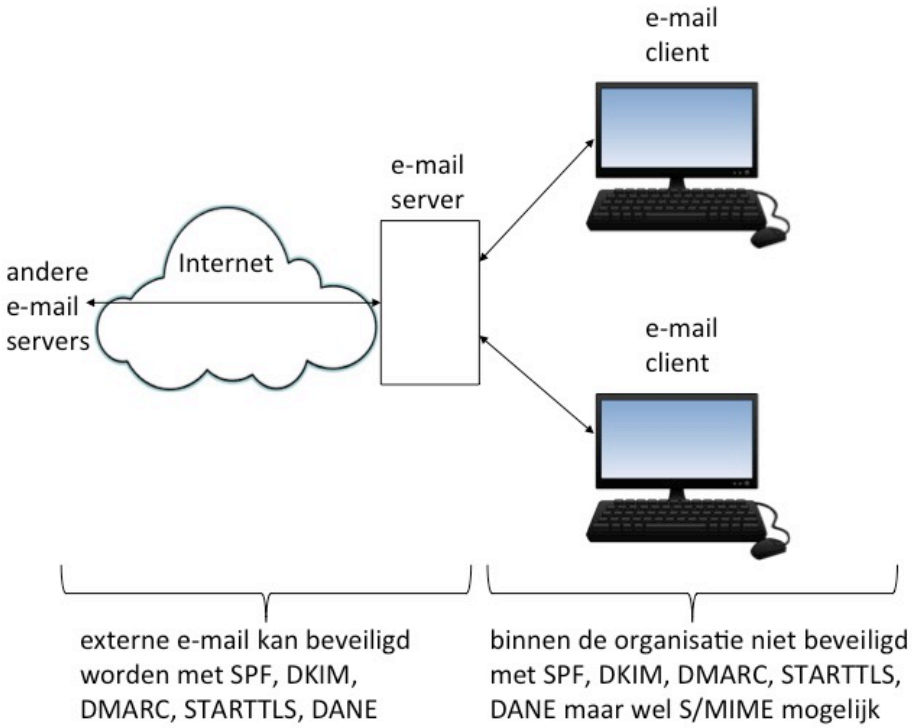
1. **Oproep aan gebruikende organisaties** voor het opstellen van een handreiking voor de implementatie/het gebruik van S/MIME bij de meest voorkomende e-mailapplicaties. Bijvoorbeeld opname op internet.nl.
2. **Oproep aan gebruikende organisaties** om een businesscase op te stellen. Dit helpt organisaties die nadenken over mogelijk gebruik van de standaard.
3. **Oproep aan softwareleveranciers** om bij webmail-omgevingen meer ondersteuning van S/MIME te bieden.

Toelichting

1. Waar gaat het inhoudelijk over?
S/MIME ondersteunt de vertrouwelijkheid en authenticiteit van e-mail uitwisseling tussen een verzendende en ontvangende e-mail client.

De verzender ondertekent zijn mail met behulp van een privésleutel die door de ontvanger (net als bij HTTPS bijvoorbeeld) op echtheid kan worden gecontroleerd. Als het certificaat vertrouwd wordt, kan de mail ook worden vertrouwd. De mail is digitaal ondertekend waardoor verandering daarin gedectecteerd kan woren. Daarnaast kan een verzender het certificaat van de ontvanger gebruiken om e-mail voor deze ontvanger te versleutelen voor verzending. De onderstaande figuren laten zien dat S/MIME e-mail beveiligt tussen eindpunten (‘end to end’). De standaard wordt met name gebruikt wanneer extra zekerheid nodig is over de veiligheid bovenop al gebruikte standaarden die tussen mailservers beveiligen (kleiner gebied) zoals SPF, DKIM, DMARC, STARTTLS en DANE.





Als de standaard niet gebruikt wordt, dan kan het voorkomen dat er misbruik wordt gemaakt van de identiteit van personen, dat e-mails gelezen of gemanipuleerd kunnen worden op het pad tussen de verzendende en ontvangende e-mail client. Als de standaard wel gebruikt wordt dan is er vanaf de cliënt (bijvoorbeeld een smartphone of een computer) veiligheid gewaarborgd, waardoor de identiteit gecontroleerd wordt. Kwaadwillenden hebben het hierdoor een stuk lastiger om hier

misbruik van te maken. Alleen als een kwaadwillende in bezit komt van de geheime sleutel kan hier misbruik van gemaakt worden.

S/MIME kan bescherming bieden in een situatie waarin veiligheidsmaatregelen zoals SPF, DKIM, DMARC, STARTTLS en DANE ontbreken of wanneer de integriteit van de mailservers niet vertrouwd kan worden. S/MIME kan zowel in combinatie met SPF, DKIM, DMARC, STARTTLS en DANE als alleenstaand gebruikt worden.

2. Hoe is het proces verlopen?

De procedurebegeleider heeft op 3 november 2017 een intakegesprek gevoerd met de indiener. Tijdens de intake is de standaard getoetst op criteria voor het in procedure nemen en is een eerste inschatting gemaakt van de kansrijkheid van de procedure. Op basis van de intake heeft het Forum Sandaardisatie op 13 december 2017 besloten de aanmelding in procedure te nemen. Hierop volgend zijn experts benaderd. Op basis van de aanmelding en de intake is een concept expertadvies opgesteld voor de experts. De procesbegeleider heeft een concept van dit expertadvies aan de leden van de expertgroep gestuurd met verzoek om commentaar. Na verwerking van reacties is het rapport nogmaals toegestuurd aan de experts, afgerond en ingediend bij het Bureau Forum Standaardisatie (het secretariaat van het Forum Standaardisatie) ten behoeve van de publieke consultatieronde. Het expertadvies is vervolgens van 23 februari – 23 maart 2018 beschikbaar gesteld voor publieke consultatie. VNG, DICTU en SURFnet hebben tijdens de openbare consultatie een reactie gegeven op het expertadvies van S/MIME.

3. Hoe scoort de standaard op de toetsingscriteria?

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.

Toegevoegde waarde

S/MIME heeft meerwaarde als een hoog beveiligingsniveau nodig is bij e-mailverkeer. Vergeleken met SPF, DKIM, DMARC, STARTTLS en DANE (die al op de ‘pas toe of leg uit’ lijst staan) heeft S/MIME toegevoegde waarde omdat S/MIME encryptie, integriteit en identificatie waarborgt tussen e-mail client applicaties (‘*end to end*’), waar SPF, DKIM, DMARC, STARTTLS en DANE dit tussen de e-mail servers controleren. S/MIME kan zowel in combinatie met SPF, DKIM, DMARC, STARTTLS en DANE als losstaand worden ingezet.
S/MIME brengt aanzienlijke kosten met zich mee. De organisatie bepaalt zelf of de kosten van het gebruik van S/MIME opwegen tegen de voordelen. De standaard PGP biedt een alternatief voor S/MIME. De keuze tussen S/MIME en PGP wordt gemaakt op basis van de wensen van de organisatie in configuratiemogelijkheden en daardoor concurreren zij niet met elkaar.

Draagvlak

Meerdere overheidspartijen gebruiken de standaard als aanvullende beveiliging bij mailverkeer nodig is. Grote marktpartijen (bijvoorbeeld Microsoft, Apple en Google) ondersteunen S/MIME in hun e-mail applicaties. Er zijn voldoende signalen dat de overheid gebruik gaat maken van deze standaard als deze meer bekend is. Het is mogelijk om OpenPGP naast S/MIME aan te bevelen binnen de overheid omdat de twee standaarden niet als concurrenten gezien hoeven worden.

Opname bevordert de adoptie
De verwachting is dat opname van de standaard op de lijst aanbevolen standaarden de adoptie van de standaard binnen de overheid zal bevorderen.

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

4. Wat is de conclusie van de expertgroep en de consultatie?

Conclusie van de expertgroep
De expertgroep adviseert het Forum Standaardisatie en het Overheidsbreed Beleidsoverleg Digitale Overheid om S/MIME 3.2 op te nemen op de lijst met open standaarden, met de status 'aanbevolen'.

Eventuele aanvullingen vanuit de consultatie
Tijdens de openbare consultatie van het expertadvies zijn vier reacties ontvangen van VNG, DICTU en SURFnet (2):

1. VNG - Het nadeel dat de e-mail niet te lezen is als de privésleutel niet meer beschikbaar is zorgt ervoor dat een organisatie na moet denken hoe hier mee om te gaan. Het expertadvies wijzigt hier niet door.
   Dit argument was tijdens de review verwerkt in samenhang met andere argumenten. De interpretatie van de verwerking bleek anders te zijn dan de oorspronkelijke intentie. Dit argument moet daarmee worden meegenomen in het geheel aan argumenten.
2. DICTU - Met een aantal voorstellen is ingestemd. Deze verdere toelichting gaat in op de verschillen met het expertadvies. Deze gaan over de verplichting van PKIoverheid certificaten en dat S/MIME en OpenPGP mogelijk samen op de lijst interoperabiliteit niet ten goede komen.
   Op het eerste punt van PKIoverheid certificaten staat dit wat te stellig in het expertadvies. Er staat niet expliciet dat het verplicht is, maar er had beter kunnen staan dat de overheid het gebruik van deze certificaten nastreeft. Met S/MIME op de lijst is het niet de intentie om PKIoverheid certificaten te verplichten. Het voorstel om bijvoorbeeld via de Rijkspas gebruik te maken van S/MIME was niet ter sprake gekomen bij de totstandkoming van het expertadvies. Als dit voor lagere kosten gebruikt kan worden dan is dat van toegevoegde waarde voor het gebruik van S/MIME en daarmee ook een waardevolle toevoeging aan het advies.
   Ten aanzien van het niet ten goede komen van de interoperabiliteit bij het mogelijk aanbevelen van S/MIME en OpenPGP geven de experts aan dat de standaarden naast elkaar kunnen worden gebruikt. Zij geven aan dat de standaarden allebei op de lijst kunnen staan en daarmee gegevensuitwisseling stimuleren. Dit betekent dat de keuze voor een standaard uitwisseling met een andere organisatie niet uitsluit. Organisaties kunnen beiden standaarden gebruiken afhankelijk van de behoefte.
3. SURFnet – Paragraaf 3.5 werd niet teruggevonden in het expertadvies. Het expertadvies heeft als laatste paragraaf 3.4. Paragraaf 3.5 is toegevoegd in het consultatiedocument en geeft, anders dan een chronologie in dat document, geen verwijzing naar een paragraaf in het expertadvies. Het is daarmee een aanvullende vraag.
4. SURFnet - Voor het grootste gedeelte is de indiener het eens met het expertadvies. De vragen gaan in op het verschil tussen S/MIME en OpenPGP. Het is mogelijk dat niet alle verschillen aan bod zijn gekomen, vooral de grootste verschillen zijn hoogover beschreven. Dat de certificaten verlopen is een toevoeging die tijdens de totstandkoming van het

expertadvies nog niet aan bod was gekomen. Ook implementatieproblemen kunnen aangedragen worden als dit een nadeel is van de standaard. Eventuele problemen is alleen niet voldoende concreet om op te kunnen nemen.
Bij certificaat beheer had beter alleen beheer kunnen staan, omdat dat de vergelijking is die gemaakt wordt.
De verschillen tussen S/MIME en OpenPGP zijn in dit geval hoog over beschreven. Er is vooral ingegaan op hoe S/MIME werkt aangezien de procedure daar over gaat. In een procedure voor bijvoorbeeld OpenPGP zou OpenPGP uitgebreider worden toegelicht inclusief de verschillen met S/MIME. In dit geval is het beschreven als extra handelingen en daardoor wat veiliger.

In de opmerkingen wordt geen reden gezien om het expertadvies te herzien of om aanvullende adviezen te geven. Wel zijn de volgende opmerkingen relevant als toevoeging op de documentatie:

1. VNG – Als de privésleutel niet beschikbaar is, dan is de e-mail die daarmee ontcijferd wordt niet meer te lezen. Een organisatie moet erover nadenken hoe hiermee om te gaan, bijvoorbeeld als werknemers vertrekken of e-mail accounts worden opgeheven.
2. DICTU - Met S/MIME op de lijst aanbevolen standaarden wordt niet nagestreefd om het gebruik van PKIoverheid certificaten voor te schrijven. De Rijkspas kan een mogelijke oplossing zijn om met minder kosten toch S/MIME te gebruiken.
3. SURFnet – Een nadeel van S/MIME is dat certificaten verlopen.

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

1. **Oproep aan gebruikende organisaties** voor het opstellen van een handreiking voor de implementatie/het gebruik van S/MIME bij de meest voorkomende e-mailapplicaties. Bijvoorbeeld opname op internet.nl.
2. **Oproep aan gebruikende organisaties** om een businesscase op te stellen. Dit helpt organisaties die nadenken over mogelijk gebruik van de standaard.
3. **Oproep aan softwareleveranciers** om bij webmail-omgevingen meer ondersteuning bij implementatie van S/MIME te bieden.

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

Bijlage

- Expertadvies S/MIME 3.2: https://www.forumstandaardisatie.nl/sites/bfs/files/20180222%20Expertadvies%20S-MIME.pdf
- Reacties uit openbare consultatie S/MIME 3.2: https://www.forumstandaardisatie.nl/sites/bfs/files/20180401%20Reacties%20uit%20openbare%20consultatie%20SMIME%203.2.pdf