Forum Standaardisatie

Expertadvies S/MIME 3.2

Datum 22 februari 2018

Colofon

Projectnaam	Expertadvies S/MIME 3.2
Versienummer	1.0
Organisatie	Forum Standaardisatie Postbus 96810 2509 JE Den Haag info@forumstandaardisatie.nl
Auteur(s)	Douwe Horst (Verdonck Klooster & Associates)

Inhoud

Samenvatting en Forumadvies

Advies aan het Forum

Het advies is om S/MIME op de lijst aanbevolen standaarden op te nemen.

Waarom is opname belangrijk?
S/MIME ondersteunt de vertrouwelijkheid en authenticiteit van e-mail uitwisseling tussen een verzendende en ontvangende e-mail client. De veiligheidstandaarden zoals SPF, DKIM, DMARC, STARTTLS en DANE verzorgen veilige gegevensuitwisseling tussen e-mail servers. Tussen e-mail client en e-mail server bieden deze standaarden echter geen bescherming.

De toegevoegde waarde van S/MIME is dat kwaadwillenden geen misbruik kunnen maken van de identiteit van iemand anders, onderschepte e-mails niet kunnen lezen, en dat manipulatie van de inhoud van een e-mail kan worden gedetecteerd. De ontvanger van een met S/MIME gesigneerde e-mail is visueel in staat te herkennen dat het bericht veilig is. Net als met HTTPS laten ondersteunende e-mail clients en webmail applicaties een grafisch icoon (zegel of slotje) zien wanneer het bericht met S/MIME is ondertekend. Zelfs ontvangers zonder technische kennis van S/MIME kunnen hier gebruik van maken.

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 beheerders van de gebruikte mailservers niet volledig vertrouwd kunnen worden, of wanneer andere maatregelen voor verbindingsbeveiliging en anti-spoofing (zoals SPF, DKIM, DMARC, STARTTLS, DANE) ontbreken.

Waar gaat het inhoudelijk over?
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. S/MIME beveiligt e-mail 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.

Hoe is het proces verlopen?
Dit expertadvies geeft de uitkomst van de experts weer. 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.

Vervolg
Het Bureau Forum Stadaardisatie zal dit expertadvies openbaar maken ten behoeve van een publieke consultatie die plaatsvindt van 23 februari tot 23 maart. Eenieder kan gedurende de consultatieperiode een reactie geven op dit expertadvies. Na afsluiting van de openbare consultatie koppelt het Bureau Forum Standaardisatie de reacties terug aan de expertgroep.

Hoe scoort de standaard op de toetsingscriteria?

Toegevoegde waarde
De toegevoegde waarde van de standaard is voldoende. De standaard heeft meerwaarde als aanvullende beveiliging nodig is bij mailverkeer. De organisatie kan zelf bepalen of de kosten in dat geval opwegen tegen de voordelen. De standaard is daarmee een aanvulling op andere standaarden op de lijst die geen end-to-end veiligheid aanbieden. De keuze tussen S/MIME en PGP wordt gemaakt op basis van de eigen wensen van de organisatie in configuratiemogelijkheden en daardoor concurreren zij niet met elkaar.

Open standaardisatieproces
De experts concluderen dat het standaardisatieproces van IETF voldoende open is. 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
Het draagvlak is voldoende. Er staan grote leveraniers achter de standaard die faciliteren in de implementatie. Meerdere overheidspartijen gebruiken de standaard als aanvullende beveiliging bij mailverkeer nodig is. In die hoedanigheid zijn er voldoende positieve signalen dat de overheid gebruik gaat maken van deze standaard als er meer bekenheid is. Het is mogelijk om OpenPGP naast S/MIME aan te bevelen binnen de overheid.

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

Welke additionele adviezen zijn er ten aanzien van de adoptie van de standaard?
De expertgroep doet het Overheidsbreed Beleidsoverleg Digitale Overheid (OBDO) de aanbeveling om bij de opname op de lijst voor 'pas toe of leg uit' de volgende oproepen ten aanzien van de adoptie van S/MIME te doen:

- 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
- Oproep aan gebruikende organisaties om een businesscase op te stellen. Dit helpt organisaties die nadenken over mogelijk gebruik van de standaard.
- Oproep aan softwareleveranciers om bij webmail-omgevingen meer ondersteuning bij implementatie te bieden.

1 Doelstelling expertadvies

1.1 Achtergrond

De Nederlandse overheid streeft naar betrouwbare gegevensuitwisseling door het gebruik van open standaarden en het voorkomen van vendor lock-in. Het actieplan "Open Overheid", de Digitale Agenda 2017 en de kabinetsreactie op het Rapport Elias benadrukken dit beleid. Om dit doel te bereiken, onderstrepen het instellingsbesluit van het Forum Standaardisatie, de Generieke Digitale Infrastructuur en de verschillende architectuurkaders het gebruik van open standaarden bij het ontwerpen of inkopen van informatiesystemen.

Een van de maatregelen om de adoptie van open standaarden te bevorderen is de publicatie en het beheer van een lijst met open standaarden waarvoor een 'pas toe of leg uit' verplichting geldt of waarvan het gebruik 'aanbevolen' is. Het Overheidsbreed Beleidsoverleg Digitale Overheid (OBDO) besluit welke standaarden op deze lijst worden opgenomen. Het OBDO baseert zich hierbij op expertadviezen, openbare consultaties en adviezen van het Forum Standaardisatie.

1.2 Doelstelling expertadvies

Dit document is een expertadvies voor S/MIME gericht aan het OBDO en Forum Standaardisatie. S/MIME is aangemeld voor opname op de lijst met open standaarden door Marco Davids van SIDN.

Doel van dit document is om het OBDO te adviseren of S/MIME in aanmerking komt voor opname op de lijst met open standaarden als aanbevolen standaard, al dan niet onder voorwaarden.

1.3 Doorlopen proces

Voor het opstellen van dit proces is de volgende procedure doorlopen:

1. De procesbegeleider heeft op 3 november 2017 een intakegesprek gevoerd met de indiener. Tijdens de intake is de standaard getoetst op criteria voor inbehandelname en is een eerste inschatting gemaakt van de kansrijkheid van de procedure.
2. 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.
3. Dit expertadvies geeft de uitkomst van de experts weer. 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.

1.4 Vervolg

Het Bureau Forum Stadaardisatie zal dit expertadvies openbaar maken ten behoeve van een publieke consultatie die plaatsvindt van 23 februari tot 23 maart. Eenieder kan gedurende de consultatieperiode een reactie geven op dit expertadvies. Na afsluiting van de openbare consultatie

koppelt het Bureau Forum Standaardisatie de reacties terug aan de expertgroep.

Het Forum Standaardisatie stelt met het expertadvies en de relevante inzichten uit de openbare consultatie een advies aan het OBDO op. Het OBDO besluit met dit advies om de standaard wel of niet op de lijst open standaarden te plaatsen.

1.5 Samenstelling expertgroep

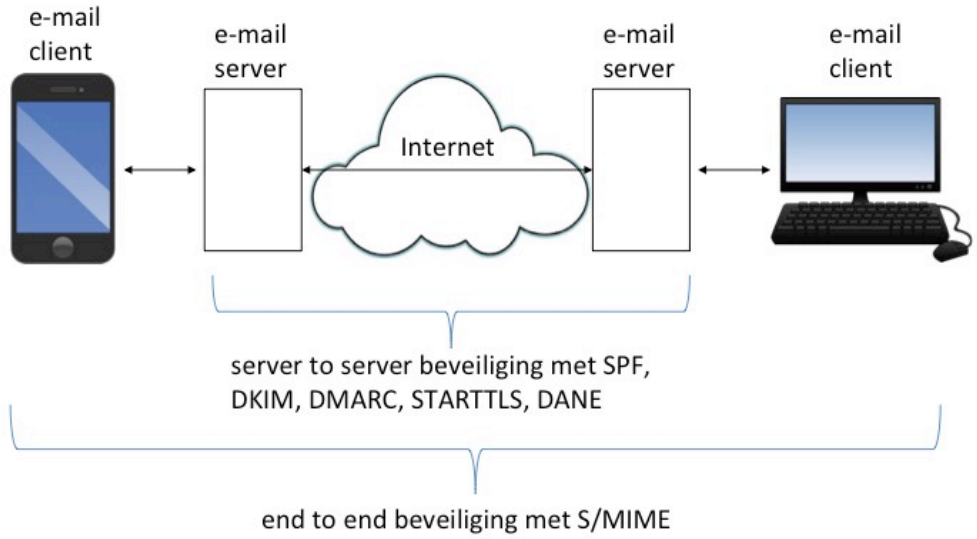
Het Forum Standaardisatie streeft naar een representatieve samenstelling van experts met een evenwichtige vertegenwoordiging van (toekomstige) gebruikers (zowel publiek als privaat), leveranciers, wetenschappers en andere belanghebbenden.

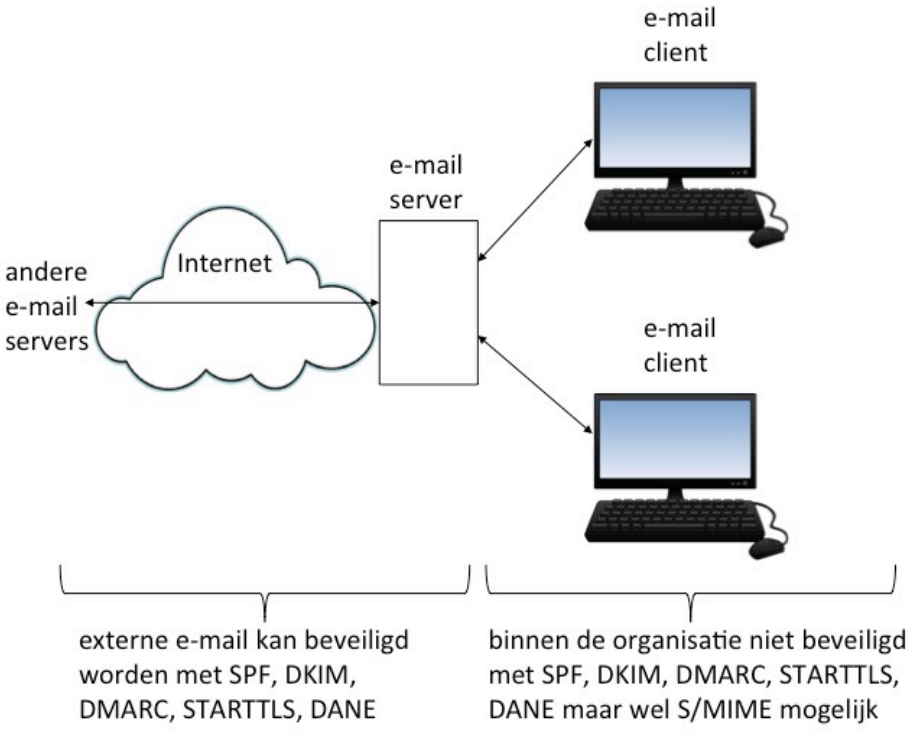
De experts zijn:
- Alwin de Bruin (Dmarcian)
- Haaino Beljaars (VNG)
- Pieter Rogaar (NCSC)
- John van Huijgevoort (IBD)
- Michel Zoetebier (KPN)
- Marco Davids (SIDN)

1.6 Toelichting S/MIME

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 beheerders van de gebruikte mailservers niet volledig vertrouwd kunnen worden, of wanneer andere maatregelen voor verbindingsbeveiliging en anti-spoofing (zoals SPF, DKIM, DMARC, STARTTLS, DANE) ontbreken.

Relatie met andere standaarden
Er is raakvlak tussen S/MIME en andere beveiligingsstandaarden voor mail. Het gaat om SPF, DKIM, DMARC, STARTTLS en DANE. De standaard kan als aanvulling gebruikt worden naast deze standaarden. S/MIME biedt end-to-end beveiliging waar de bovengenoemde standaarden beveiliging tussen mailservers (server-to-server) geven. S/MIME kan worden gebruikt wanneer aanvullende beveiliging nodig is op die van SPF, DKIM, DMARC, STARTTLS en DANE.

S/MIME heeft met name een relatie met de 'aanbevolen' standaard MIME op de lijst met open standaarden. S/MIME zorgt voor veilig verkeer van MIME en is daarmee een toevoeging bij het gebruik van MIME.

S/MIME heeft daarnaast een relatie met OpenPGP, een standaard die vergelijkbaar is met S/MIME. S/MIME wordt door de experts als gebruiksvriendelijker gezien: OpenPGP vereist extra handelingen bij het certificaatbeheer. Tegelijkertijd is OpenPGP daardoor ook wat veiliger. Ondanks deze verschillen lijken de standaarden aanzienlijk op elkaar. De standaarden kunnen allebei gebruikt worden maar kennen een andere gebruiksgroep. OpenPGP wordt meer gebruikt door mensen met specialistische kennis en als er behoefte is meer instellingen naar eigen invulling in te richten. Experts geven aan dat de standaarden niet met elkaar concurreren. Naast het aanbevolen stellen van S/MIME kan OPenPGP in potentie ook op de lijst worden opgenomen.

1.7 Leeswijzer

Hoofdstuk 2 beschrijft het functioneel toepassingsgebied (situaties waarin de standaard functioneel gebruikt moet worden) en hetorganisatorisch werkingsgebied (organisaties die de standaard moeten toepassen).

Hoofdstuk 3 beschrijft de resultaten van de toetsing van de standaard aan de hand van de criteria voor opname op de lijst open standaarden.

2 Toepassings– en werkingsgebied

De *instructie rijksdienst inzake de aanschaf van ICT producten en ICT diensten* verplicht overheidsorganisaties om relevante standaarden op de 'pas toe of leg uit te vragen en toe te passen bij aanbestedingstrajecten.

Afhankelijk van de aan te schaffen functionaliteit moet een overheidsorganisatie bepalen welke standaarden op de 'pas toe of leg uit' lijst relevant zijn. Hiervoor is voor iedere standaard een *functioneel toepassingsgebied* (in welke situaties is de standaard functioneel van toepassing) en een *organisatorisch toepassingsgebied* (welke oranisaties moeten de standaard gebruiken) beschreven.

Secties 2.1 en 2.2 geven het advies van de expertgroep voor het functioneel en organisatorisch toepasingsgebied van S/MIME.

2.1 Functioneel toepassingsgebied

De expertgroep adviseert als functioneel toepassingsgebied voor S/MIME 3.2:

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.

2.2 Organisatorisch werkingsgebied

De expertgroep adviseert als organisatorisch werkingsgebied:

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.

3 Toetsing van standaard aan criteria

Het Forum Standaardisatie hanteert vier hoofdcriteria om te bepalen of een standaard in aanmerking komt voor opname op de lijst:
1. Heeft de standaard toegevoegde waarde?
2. Zijn de standaard en het standaardisatieproces voldoende open?
3. Heeft de standaard voldoende draagvlak?
4. Is opname op de lijst nodig om de adoptie te bevorderen?[1]

Ieder van deze hoofdcriteria heeft deelcriteria die beschreven staan in het document *"Toetsingsprocedure en criteria voor lijst met open standaarden voor indieners en experts",* te vinden op de website van het Forum Standaardisatie https://www.forumstandaardisatie.nl/content/toetsen-van-standaarden.

Dit hoofdstuk beschrijft per criterium het resultaat van de toetsing. Voor de volledigheid is tevens de beschrijving 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.

3.1.1 Is het toepassings- en werkingsgebied van de aanmelding goed gedefinieerd?

3.1.1.1 Is het functioneel toepassingsgebied goed gedefinieerd?
Zie §2.1.

3.1.1.2 Is het organisatorisch werkingsgebied goed gedefinieerd?
Zie §2.2

3.1.1.3 Is de standaard generiek toepasbaar (en niet alleen bedoeld voor gegevensuitwisseling met één of een beperkt aantal specifieke organisaties)? (toelichtende vraag)
Ja, de standaard is generiek toepasbaar. Het kan gaan om een beperkt aantal specifieke organisaties. De toepasbaarheid hangt af van het aantal organisaties dat het nodig vindt om aanvullende beveiligingsmaatregelen bij e-mail te treffen.

3.1.2 Verhoudt de standaard zich goed tot andere standaarden?

3.1.2.1 Kan de standaard naast of in combinatie met reeds opgenomen standaarden worden toegepast (d.w.z. de standaard conflicteert niet met reeds opgenomen standaarden)?
Ja, er is raakvlak tussen S/MIME en andere beveiligingsstandaarden voor mail. Het gaat om SPF, DKIM, DMARC, STARTTLS en DANE. De standaard kan als aanvulling gebruikt worden naast deze standaarden.

1 Dit criterium is voornamelijk van toepassing op standaarden op de 'pas toe of leg uit' lijst, niet voor aanbevolen standaarden.

3.1.2.2 Biedt de aangemelde standaard meerwaarde boven reeds opgenomen standaarden met een overlappend functioneel toepassings- en organisatorisch werkingsgebied? (Dit kan ook om een nieuwe versie van dezelfde standaard gaan.)
Ja, de meerwaarde zit in de beveiliging tussen eindpunten (end-to-end), waar de in 3.1.2.1 genoemde standaarden beveiliging tussen e-mail servers bieden. De belangrijkste overlap is er met de 'aanbevolen' standaard MIME op de lijst met open standaarden. S/MIME zorgt voor veilig verkeer van MIME en is daarmee een toevoeging bij het gebruik van MIME.

3.1.2.3 Biedt de aangemelde standaard meerwaarde boven bestaande concurrerende standaarden die in aanmerking zouden kunnen komen voor opname? (toelichtende vraag)
Ja, S/MIME heeft een relatie met OpenPGP, een standaard die vergelijkbaar is met S/MIME. S/MIME wordt door de experts als gebruiksvriendelijker gezien: OpenPGP vereist extra handelingen bij het certificaatbeheer. Tegelijkertijd is OpenPGP daardoor ook wat veiliger. Ondanks deze verschillen lijken de standaarden aanzienlijk op elkaar. De standaarden kunnen allebei gebruikt worden maar kennen een andere gebruiksgroep. OpenPGP wordt meer gebruikt door mensen met specialistische kennis en als er behoefte is meer instellingen naar eigen invulling in te richten. Experts geven aan dat de standaarden niet met elkaar concurreren. Naast het aanbevolen stellen van S/MIME kan OPenPGP in potentie ook op de lijst worden opgenomen.

3.1.2.4 Is de standaard een internationale standaard of sluit de standaard aan bij relevante internationale standaarden? (toelichtende vraag)
Ja, S/MIME wordt beheerd door de Internet Engineering Task Force (IETF). IETF is een internationale standaardisatieorganisatie voor internetstandaarden. IETF beheert onder andere ook DKIM, DNSSEC, HTTPS en HSTS, IPv6 en IPv4, SPF, STARTTLS en DANE en TLS met de status 'pas toe of leg uit' op de lijst open standaarden. Daarnaast zijn er tal van standaarden met de status 'aanbevolen op de lijst'.

3.1.3 Wegen de kwantitatieve en kwalitatieve voordelen van adoptie van de standaard, voor de (semi-)overheid als geheel en voor de maatschappij, op tegen de nadelen?
Ja, maar het grootste nadeel zijn de bijkomende kosten. Ieder persoon die gebruik wil maken van S/MIME moet over een sleutelpaar beschikken en het bijbehorende digitale certificaat met de publieke sleutel die anderen kunnen gebruiken om de e-mail te verifiëren. Een organisatie moet zelf bepalen of de mate van beveiliging nodig is. Als dat het geval is dan kan een organisatie de keuze maken of de voordelen opwegen tegen de nadelen. Een ander nadeel kan ook zijn dat personen steeds meer apparaten hebben en dat het voor gebruikers gemakkelijk moet zijn om met alle apparaten de standaard te gebruiken. Dit zit in de extra beheerlast die verderop is beschreven.

3.1.3.1 Zijn de kosten van implementatie acceptabel en zijn deze kosten bekend en inzichtelijk?
Ja, de kosten voor certificaten zijn ongeveer 150 euro per certificaat per 2 jaar (zie bijvoorbeeld https://www.globalsign.com/en/personalsign/pricing/) Bij grootafname worden deze kosten lager. Binnen de overheid is afgesproken dat voor interne en externe communicatie in principe alleen gebruik gemaakt mag

worden van PKIoverheid certificaten. De kosten per jaar zijn ongeveer 120 euro voor persoonsgebonden digitale certificaten. De voordelen wegen op tegen de kosten als een organisatie het van het belang acht meer beveiligingsmaatregelen binnen mailverkeer toe te passen. S/MIME vergt extra beheerslast, maar er kan voor gekozen worden om S/MIME alleen in bepaalde gevallen te gebruiken. Bijvoorbeeld in mails waarvan de authenticiteit van afzender van groot belang is, of waarbij de vertrouwelijkheid van de mail hoog is. Het gebruik kan gekoppeld worden aan rollen of functies. Denk voor gemeenten bijvoorbeeld aan het college van B&W en raadsleden, medewerkers van specifieke diensten waar vertrouwelijkheid belangrijk is. Naast rol gebonden kan ook een keuze gemaakt worden voor S/MIME als dat nodig is voor de inhoud van het bericht. Het is aan de verstuurder van het bericht om daar een risico inschatting van te maken.

3.1.3.2 Is er een (kwalitatieve) businesscase van de standaard aanwezig?
Nee, er is geen businesscase van de standaard aanwezig. Dit komt door het beperkte gebruik van S/MIME binnen de overheid.

3.1.3.3 Is de meerwaarde van de standaard goed inzichtelijk te maken? Wat betekent de standaard voor de (bedrijfs)processen van een organisatie of keten en wat los je met de standaard op?
S/MIME ondersteunt de vertrouwelijkheid en authenticiteit van e-mail uitwisseling tussen een verzendende en ontvangende e-mail client. De veiligheidstandaarden zoals SPF, DKIM, DMARC, STARTTLS en DANE verzorgen veilige gegevensuitwisseling tussen e-mail servers. Tussen e-mail client en e-mail server bieden deze standaarden echter geen bescherming. De meerwaarde van S/MIME is dat kwaadwillenden geen misbruik kunnen maken van de identiteit van iemand anders, onderschepte e-mails niet kunnen lezen, en dat manipulatie van de inhoud van een e-mail kan worden gedetecteerd. De ontvanger van een met S/MIME gesigneerde e-mail is visueel in staat te herkennen dat het bericht veilig is. Net als met HTTPS laten ondersteunende e-mail clients en webmail applicaties een grafisch icoon (zegel of slotje) zien wanneer het bericht met S/MIME is ondertekend. Zelfs ontvangers zonder technische kennis van S/MIME kunnen hier gebruik van maken.

3.1.3.4 Zijn de beveiligingsrisico's aan overheidsbrede adoptie van de standaard acceptabel?
Ja, de risico's zijn acceptabel. Een mogelijk beveiligingsrisico is dat wanneer een derde partij toegang krijgt tot een geheime sleutel (door slordigheid, diefstal of kraken), deze alle historisch uitgewisselde e-mails kan ontcijferen. Dit risico kan worden beperkt door tijdig/regelmatig van certificaat te wisselen, bijvoorbeeld jaarlijks. Voor veel organisaties wegen de voordelen van de standaard op tegen het risico van sleutelverlies.

3.1.3.5 Zijn de privacyrisico's aan overheidsbrede adoptie van de standaard acceptabel?
Ja, er zijn geen bijkomende privacyrisico's te benoemen. De standaard draagt zelfs bij aan de vertrouwelijkheid van berichten.

3.1.4 Conclusie criteria 'Toegevoegde waarde'

De toegevoegde waarde van de standaard is voldoende. De standaard is van meerwaarde als aanvullende beveiliging nodig is bij mailverkeer. De organisatie kan zelf bepalen of de kosten in dat geval opwegen tegen de

voordelen. De standaard is daarmee een aanvulling op andere standaarden op de lijst die minder breed encryptie aanbieden. De keuze tussen S/MIME en PGP wordt gemaakt op basis van de eigen wensen van de organisatie in configuratiemogelijkheden en daardoor concurreren zij niet met elkaar.

3.2 Open standaardisatieproces

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

3.2.1 Is de documentatie voor een ieder drempelvrij beschikbaar?

3.2.1.1 Is het specificatiedocument beschikbaar zonder dat er sprake is van belemmeringen (zoals hoge kosten of lidmaatschapseisen)?
Ja, dit is beschikbaar zonder belemmeringen:
https://tools.ietf.org/html/rfc5751

3.2.1.2 Is de documentatie over het ontwikkel- en beheerproces (bijv. het voorlopige specificatiedocument, notulen en beschrijving van de besluitvormingsprocedure) beschikbaar zonder dat er sprake is van belemmeringen (zoals hoge kosten of lidmaatschapseisen)?
Ja, de documentatie over het ontwikkel- en beheerproces is gratis en voor iedereen te downloaden via de website van IETF. De specificatiedocumenten zijn gepubliceerd op de website van IETF.

Specificaties doorlopen in het standaardisatieproces van IETF twee stadia van volwassenheid: 'proposed standard' en 'internet standard'. De voortgang van door IETF beheerde standaarden in dit proces is transparant en kosteloos te volgen via de RFC's van de standaarden. RFC 5751 is een 'proposed standard'.

Overige documentatie zoals notulen van bijeenkomsten en besluiten zijn ook kosteloos beschikbaar op de website van IETF.

3.2.2 Is het intellectuele eigendomsrecht voor eenieder beschikbaar, zodat de standaard vrij implementeerbaar en te gebruiken is?

3.2.2.1 Stelt de standaardisatieorganisatie het intellectueel eigendomsrecht op de standaard (bijvoorbeeld patenten of licenties) onherroepelijk royalty-free voor eenieder beschikbaar?
Ja, de Intellectual Property Rights (IPR) van IETF is vastgelegd in RFC3979. Hierin staat dat leden van de werkgroep van een specifieke standaard bestaande en relevante IPR moeten bekendmaken. Voor S/MIME zijn geen IPR geclaimd waardoor dit inderdaad voor eenieder beschikbaar is.

3.2.2.2 Garandeert de standaardisatieorganisatie dat partijen die bijdragen aan de ontwikkeling van de standaard hun intellectueel eigendomsrecht voor (onderdelen van) de standaard onherroepelijk royalty-free voor eenieder beschikbaar stellen?
Nee, dat er bij inbeheername van standaarden door IETF geen IPR is geclaimd geeft geen garantie over toekomstige claims met betrekking tot het intellectueel eigendom.

3.2.3 Is de inspraak van eenieder in voldoende mate geborgd?

3.2.3.1 Is het besluitvormingsproces toegankelijk voor alle belanghebbenden (bijv. gebruikers, leveranciers, adviseurs, wetenschappers)?
Ja, verschillende werkgroepen werken aan de (door)ontwikkeling van IETF-standaarden. Samenwerking binnen deze werkgroepen vindt veelal plaats via e-mail. Belanghebbenden zoals gebruikers, leveranciers, adviseurs en wetenschappers kunnen zich via de website van IETF aanmelden voor de mailinglijsten van werkgroepen. Hier zijn geen (lidmaatschaps)kosten aan verbonden.

3.2.3.2 Vindt besluitvorming plaats op een wijze die zoveel mogelijk recht doet aan de verschillende belangen?
Ja, het standaardisatieproces van IETF maakt gebruik van een besluitvormingsprocedure via het principe van 'rough consensus', waarbij de dominante mening van een groep, zoals door de voorzitter vastgesteld, de basis voor een beslissing vormt.

3.2.3.3 Kan een belanghebbende formeel bezwaar aantekenen tegen de gevolgde procedure?
Ja, binnen de werkgroepen kunnen belanghebbenden bezwaren kenbaar maken. Buiten de werkgroepen kan bezwaar worden aangetekend bij de leden van de Internet Engineering Steering Group (IESG).

3.2.3.4 Organiseert de standaardisatieorganisatie regelmatig overleggen met belanghebbenden over doorontwikkeling en beheer van de standaard?
Ja, belanghebbenden kunnen zich aanmelden voor werkgroepen die werken aan de doorontwikkeling van standaarden. Er wordt veelvuldig gebruik gemaakt van mailingslists waarvoor een ieder zich kan aanmelden.

3.2.3.5 Organiseert de standaardisatieorganisatie een publieke consultatie voordat (een nieuwe versie van) de standaard wordt vastgesteld?
Ja, IETF werkt met RFC's, het standaard publicatieformaat voor Internet Standaarden van IETF. Voordat een nieuwe RFC van een standaard wordt geaccordeerd, wordt door een werkgroep van deze standaard een zogeheten open comments proces georganiseerd waarbij belanghebbenden commentaar kunnen leveren over de (nieuwe versie van de) standaard.

3.2.4 Is de standaardisatieorganisatie onafhankelijk en duurzaam?

3.2.4.1 Is de ontwikkeling en het beheer van de standaard belegd bij een onafhankelijke non-profit standaardisatieorganisatie?
Ja, IETF is een onafhankelijke organisatie zonder winstoogmerk.

3.2.4.2 Is de financiering van de ontwikkeling en het onderhoud van de standaard voor tenminste drie jaar gegarandeerd?
Ja, de financiering van de ontwikkeling en het onderhoud van de standaard wordt verzorgd door de leden van de werkgroep waar de standaarden onder vallen. IETF bestaat meer dan 30 jaar en heeft zich in het verleden bewezen als stabiele standaardisatieorganisatie. De experts zijn om deze reden van mening dat de continui¨teit van de financiering voor IETF- standaarden hierdoor voldoende is gewaarborgd.

3.2.5 Is het (versie) beheer van de standaard goed geregeld?

3.2.5.1 Heeft de standaardisatieorganisatie gepubliceerd beleid met betrekking tot (versie)beheer van de standaard? Bij voorkeur is dit beleid ook beschreven in een beheerplan (met o.a. aandacht voor migratie van gebruikers)
Ja, de inhoud van eerdere versies van IETF-standaarden is terug te lezen op de website van IETF. In de verschillende RFC's van een standaard is aandacht voor de implementatie van een standaard.

3.2.5.2 Is de beheerdocumentatie goed vindbaar en verkrijgbaar?
Ja, de beheerdocumentatie is goed vindbaar en verkrijgbaar: https://tools.ietf.org/html/rfc5751

3.2.5.3 Is het belang van de Nederlandse overheid voldoende geborgd bij de ontwikkeling en het beheer van de standaard?
Ja, de Nederlandse overheid kan zich, indien gewenst, aanmelden voor deelname aan de werkgroepen. Voor zover bekend heeft de Nederlandse overheid geen betrokkenheid gehad bij de ontwikkeling of het beheer van de standaard.

3.2.5.4 Is de vertegenwoordiging van belanghebbenden bij het beheer van de standaard een goede representatie van het werkingsgebied en functioneel toepassingsgebied van de standaard?
Ja, iedere belanghebbende kan een bijdrage leveren aan het beheer van de standaard.

3.2.5.5 Is het standaardisatieproces van de standaardisatieorganisatie zodanig goed geregeld dat het Forum zich kan onthouden van aanvullende toetsing bij de aanmelding van een nieuwe versie van de standaard?
Nee. Hoewel IETF een solide en open beheerproces heeft, is het predicaat 'uitstekend beheer' niet van toepassing op IETF standaarden.

3.2.6 Is er adoptieondersteuning voor de standaard?

3.2.6.1 Is er een toegankelijk aanspreekpunt of organisatie waar meer informatie over de standaard is te vinden en op te vragen is?
Ja, IETF is het aanspreekpunt waar vragen te stellen zijn en gemakkelijk informatie over de standaard is te vinden.

3.2.6.2 Wordt er ondersteuning gegeven in de adoptie en de implementatie van de standaard?
Ja, er is ondersteuning in het gebruik van de standaard vanuit IETF, waar een community bestaat. Er wordt ondersteuning gegeven in de adoptie van de standaard door grote softwareleveranciers zoals Microsoft, Apple, Mozilla en Google.

3.2.7 Conclusie criteria 'Open standaardisatieproces'

De experts concluderen dat het standaardisatieproces van IETF voldoende open is. 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.

3.3 Draagvlak

Aanbieders en gebruikers moeten voldoende positieve ervaring met de standaard hebben.

3.3.1 Bestaat er voldoende marktondersteuning voor de standaard?

3.3.1.1 Bieden meerdere leveranciers ondersteuning voor de standaard?
Ja, grote softwareleveranciers zoals Microsoft, Apple, Mozilla en Google bieden ondersteuning voor de standaard. Met name bij webmail-omgevingen die S/MIME niet al ondersteunen kan het nog weleens uitdagend zijn om de standaard te implementeren.

3.3.1.2 Kan een gebruiker de conformiteit van de implementatie van de standaard (laten) toetsen?
Ja, leveranciers bieden ondersteuning bij de implementatie en de conformiteit daarvan, zoals Mozilla https://www-archive.mozilla.org/projects/security/pki/psm/smime_guide.html en Microsoft https://blogs.msdn.microsoft.com/jasonlan/2007/11/06/smime-implementation-guide/.

3.3.1.3 Draagt de standaard voldoende bij aan interoperabiliteit zonder dat aanvullende standaardisatieafspraken (zoals lokale profielen) noodzakelijk zijn om de standaard te implementeren of te gebruiken?
Ja, het is niet vanzelfsprekend om de standaard te implementeren maar er zijn geen aanvullende standaardisatieafspraken noodzakelijk om de standaard te implementeren of te gebruiken. Er is wel een zekere beheerslast zoals eerder beschreven.

3.3.1.4 Zijn er profielen of voorbeeldimplementaties van de standaard aanwezig en zijn deze vrij te gebruiken?
Ja, er zijn diverse voorbeeldimplementaties te vinden, waaronder bijvoorbeeld https://www.ipa.go.jp/security/rfc/RFC4134EN.html.

3.3.2 Kan de standaard rekenen op voldoende draagvlak?

3.3.2.1 Staan de belangrijkste stakeholders vanuit de overheid voor deze standaard achter de adoptie van de standaard?
Nee, hier is onvoldoende over bekent. Vooralsnog staan SIDN en het Ministerie van Defensie achter het gebruik van de standaard. De experts verwachten dat meer organisaties de standaard willen ondersteunen.

3.3.2.2 Staan de overheidsorganisaties die daadwerkelijk worden geraakt door een mogelijke verplichting van de standaard achter het gebruik van de standaard?
Ja, want er is in dit geval geen sprake van een verplichting.

3.3.2.3 Wordt de aangemelde versie van de standaard binnen het organisatorische werkingsgebied door meerdere Nederlandse overheidsorganisaties gebruikt?
Ja, SURFnet, het Ministerie van Defensie, het Miniserie van Algemene Zaken en enkele gemeenten maken ervan gebruik.

3.3.2.4 Wordt een vorige versie van de standaard binnen het organisatorische werkingsgebied door meerdere Nederlandse overheidsorganisaties gebruikt?
Nee, hier is onvoldoende zicht op.

3.3.2.5 Is de aangemelde versie backwards compatible met eerdere versies van de standaard?
Ja, de standaard is backwards compatible met eerdere versies. Voor sterk verouderde e-mailapplicaties geldt dat S/MIME beperkt ondersteund wordt. Deze sterk verouderde applicaties ondersteunen tevens geen andere vormen van moderne e-mail beveiliging: https://tools.ietf.org/html/rfc5751#section-1.4

3.3.2.6 Zijn er voldoende positieve signalen over toekomstige gebruik van de standaard door (semi-)overheidsorganisaties, het bedrijfsleven en burgers?
Ja, een aanvullende beveiliging bij mailverkeer is een overweging die maken aangezien organisaties schending van privacy door kwaadwillenden willen tegengaan. Tegelijkertijd wordt er ook naar alternatieve kanalen gezocht voor het uitwisselen van vertrouwelijke informatie, zoals end-to-end-encrypted chat applicaties.

3.3.3 Conclusie criteria 'Draagvlak'

Het draagvlak is voldoende. Er staan grote leveraniers achter de standaard die faciliteren in de implementatie. Meerdere overheidspartijen gebruiken de standaard als aanvullende beveiliging bij mailverkeer nodig is. In die hoedanigheid zijn er voldoende positieve signalen dat de overheid gebruik gaat maken van deze standaard als er meer bekenheid is. Daarnaast is mogelijk ook OpenPGP aan te bevelen binnen de overheid.

3.4 Opname bevordert adoptie

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

Met de lijst wil het OBDO de adoptie van open standaarden bevorderen die voldoen aan de voorgaande criteria (toegevoegde waarde, standaardisatieproces en draagvlak).
- Met de "pas toe of leg uit"-status beoogt het OBDO standaarden te verplichten als:
  a. hun huidige adoptie binnen de (semi-)overheid beperkt is;
  b. opname op de lijst bijdraagt aan de adoptie door te stimuleren (functie = stimuleren).
- Met de aanbevolen standaarden beoogt het OBDO standaarden aan te bevelen als :
  a. hun huidige adoptie binnen de (semi-)overheid reeds hoog is;
  b. opname op de lijst bijdraagt aan de adoptie door te informeren en daarmee onbedoelde afwijkende keuzes te voorkomen (functie = informeren).

3.4.1 Is "pas toe of leg uit" het passende middel om de adoptie van de standaard binnen de (semi)overheid te bevorderen?

Nee, een verpichting niet aan de orde gezien de beheerlast in relatie tot de meerwaarde van de e-mail veiligheidstandaarden die al op de 'pas toe of leg uit' lijst staan. Daarnaast kan S/MIME niet zonder meer verplicht

worden zonder ook PGP in overweging te nemen. S/MIME en PGP kunnen wel naast elkaar worden gebruikt als aanbevolen standaarden.

3.4.2 Is de status "aanbevolen" het passende middel om de adoptie van de standaard binnen de (semi)overheid te bevorderen?

Ja, met name organisaties die aanvullende beveiliging bij mailverkeer nastreven zullen baat hebben bij het gebruik van S/MIME. Een verplichting is voor deze groep niet nodig.

3.4.3 Conclusie criteria 'Opname bevordert adoptie'

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

3.4.4 Adoptieactiviteiten

Gebruik van de standaard is het einddoel van het Forum Standaardisatie en OBDO. Plaatsing op de lijst met open standaarden 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?

De expertgroep adviseert het OBDO om bij de opname op de lijst voor 'pas toe of leg uit' de volgende oproepen ten aanzien van de adoptie van S/MIME te doen:

- 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
- Oproep aan gebruikende organisaties om een businesscase op te stellen. Dit helpt organisaties die nadenken over mogelijk gebruik van de standaard.
- Oproep aan softwareleveranciers om bij webmail-omgevingen meer ondersteuning bij implementatie te bieden.