Forum Standaardisatie

Wilhelmina van Pruisenweg 52
2595 AN Den Haag

Postbus 96810
2509 JE Den Haag

www.forumstandaardisatie.nl

notitie

FORUM STANDAARDISATIE 13 december 2017

Agendapunt:	4F		
Betreft:	Concept intake-advies voor S/MIME		
Aan:	Stuurgroep open standaarden		
Van:	Bureau Forum Standaardisatie		
Datum:	21 november 2017	**Versie**	0.2

Advies

Het Forum Standaardisatie wordt geadviseerd om Secure/Multipurpose Internet Mail Extensions (hierna: S/MIME) versie 3.2 in behandeling te nemen voor opname op de lijst met open standaarden met de status 'aanbevolen'.

In procedure nemen van deze standaard is van belang vanwege de extra veiligheid die deze standaard ten opzichte van andere standaarden levert door middel van end-to-end encryptie bij het gebruik van e-mail. Opname op de lijst stimuleert de verdere adoptie van de standaard.

Over S/MIME
De verzender ondertekend en/of versleuteld zijn mail met behulp van een certificaat dat 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 en zodoende beschermd tegen wijzigen. 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.

Korte toelichting advies
De standaard voldoet aan de criteria voor inbehandelname als 'aanbevolen' standaard. S/MIME is een standaard die gebruikt wordt om elektronische gegevensuitwisseling tussen mailclients te beveiligen. De standaard is niet wettelijk verplicht. De standaard lost het probleem op dat wanneer de hoogste categorie van beveiliging nodig is bij mailverkeer beveiliging van begin tot eind is gewaarborgd. Bij andere standaarden is deze beveiliging

minder breed waardoor binnen dezelfde mailserver alsnog een andere identiteit kan worden aangenomen. Een nadeel is dat bij het verkrijgen van de sleutel door een derde de historie ook inzichtelijk is aangezien daar dezelfde sleutel voor wordt gebruikt.

De kansrijkheid van de standaard is voldoende. De eerste inschatting van het open standaardisatieproces, toegevoegde waarde en opname bevordert adoptie is positief. Met name het draagvlak is nog onvoldoende duidelijk, het is namelijk niet duidelijk welke overheden de standaard gebruiken en of zij de aanmelding willen ondersteunen. Dit moet uitgezocht worden tijdens de procedure.

Er is raakvlak tussen S/MIME en andere encryptiestandaarden voor mail. Een sterke relatie is er met Pretty Good Privacy (hierna: PGP), een standaard die vergelijkbaar is met S/MIME maar lastiger in gebruik is en minder softwareondersteuning kent. Toch lijken beide standaarden gebruikt te worden en is de vraag wat de verschillen precies zijn in het gebruik.

Toelichting

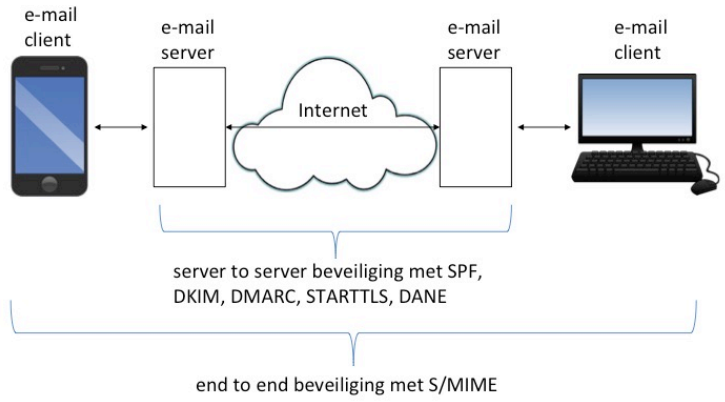
1. Aanmelding, intakegesprek en toetsingsprocedure

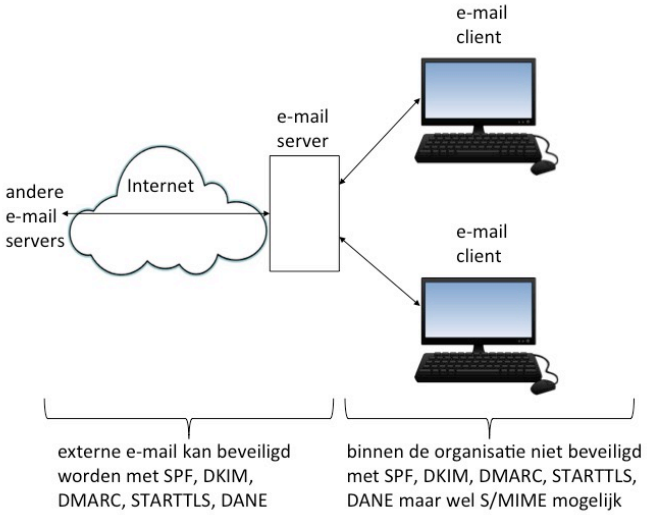
Op 24 oktober 2017 is door Marco Davids van SIDN een standaard aangemeld, betreffende aanmelding versie 3.2 van S/MIME voor de lijst met open standaarden. De aanmelder heeft als doel de standaard een 'aanbevolen' standaard te maken.

Op 3 november 2017 heeft een intakegesprek plaatsgevonden met de aanmelder. In dit gesprek is de aanmelding besproken. Hierbij is gekeken of alle basisinformatie aanwezig is en of de standaard voldoet aan de criteria voor inbehandelname. Daarnaast is vooruitgeblikt op de procedure.

2. Korte beschrijving standaard

Waar gaat S/MIME over?





De verzender ondertekend en/of versleuteld zijn mail met behulp van een certificaat dat 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 en zodoende beschermd tegen wijzigen. In bovenstaande afbeeldingen is te zien dat de mail van begin tot eind (end-to-end) met encryptie beveiligd is. Juist binnen de organisatie is die extra beveiliging van toepassing. 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.

Welk probleem lost de standaard op?
De standaard lost het probleem op dat wanneer de hoogste categorie van beveiliging nodig is bij mailverkeer beveiliging van begin tot eind is gewaarborgd. Bij andere standaarden is deze beveiliging minder breed waardoor tussen mailserver en client (bijvoorbeeld smartphone of computer) alsnog een andere identiteit kan worden aangenomen. Het probleem dat hier daadwerkelijk mee wordt opgelost is dat kwaadwillenden geen misbruik kunnen maken van de identiteit van iemand anders en ze kunnen de onderschepte e-mails niet lezen of wijzigen.

Wie beheert de standaard?
De standaard is in beheer bij de internationale organisatie IETF. Het standaardisatieproces van IETF is voldoende open. IETF is beheerorganisatie van meerdere standaarden die op de lijst met open standaarden staan waar dit ook getoetst 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.

Waarom is de standaard aangemeld voor aanbevolen?
De standaard is aangemeld voor de status 'aanbevolen' omdat een verplichting te zwaar is gezien de complexe aard van de standaard. Met name organisaties die de hoogste categorie van beveiliging bij mailverkeer nastreven zullen baat hebben bij de complexe implementatie van de standaard. Een verplichting is voor die groep niet het juiste middel. Daarnaast is de alternatieve standaard PGP ook in gebruik en kan S/MIME niet per definitie verplicht gesteld worden boven PGP.

(zie ook: *7. Functionele use case*)

3. Criteria voor inbehandelname

Om een standaard in behandeling te nemen moet de standaard vallen binnen de scope van de lijst. Hiervoor gelden vier criteria:

1. Is de standaard toepasbaar voor elektronische gegevensuitwisseling tussen (semi-)overheidsorganisaties en bedrijven, tussen (semi-)overheidsorganisaties en burgers of tussen (semi-)overheidsorganisaties onderling?
Ja, S/MIME is een standaard die gebruikt wordt om e-mail te beveiligen. Hiermee beslaat de standaard het volledige proces van mail uitwisseling tussen eindgebruikers (dit in tegenstelling tot SPF, DKIM en DMARC tie tussen organisaties gaan).

2. Is het beoogde functioneel toepassingsgebied en het organisatorisch werkingsgebied van de standaard, voldoende breed om substantieel bij te dragen aan de interoperabiliteit van de (semi-)overheid?
Ja, het functioneel toepassingsgebied is minder uitgebreid dan bekende standaarden als SPF, DKIM en DMARC maar de standaard is wel een aanvulling op deze standaarden bij extra beveiliging. E-mail is daarnaast voldoende breed aangezien er zeer veel gebruik wordt gemaakt van dit communicatiemiddel bij de overheid.

3. Is het zinvol de standaard op te nemen, gezien het feit dat deze niet al wettelijk verplicht is voor het beoogde functioneel toepassingsgebied en organisatorisch werkingsgebied?
Ja, de standaard is niet wettelijk verplicht.

4. Draagt de standaard bij aan de oplossing van een bestaand, relevant (interoperabiliteits)probleem en het voorkomen van leveranciersafhankelijkheid?
Ja, de standaard lost het probleem op van volledige e-mail beveiliging tussen eindgebruikers. Bij andere standaarden is deze beveiliging minder breed waardoor tussen mailserver en cliënt (bijvoorbeeld smartphone of computer) alsnog een andere identiteit kan worden aangenomen. Het probleem dat hier daadwerkelijk mee wordt opgelost is dat kwaadwillenden geen misbruik kunnen maken van de identiteit van iemand anders en dat ze e-mails niet kunnen lezen of wijzigen.

<u>Conclusie</u>
De standaard voldoet aan de criteria voor inbehandelname.

4. Toetsing kansrijkheid procedure

Het Forum Standaardisatie wil voorkomen dat er standaarden in procedure worden genomen, waarvan bij voorbaat al bekend is dat deze in de expertronde of consultatieronde zullen stranden op één van de inhoudelijke criteria. Daarom heeft de procedurebegeleider de beantwoording van de criteriavragen nagelopen, waar mogelijk zelf aangevuld en vervolgens besproken met de indiener.

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

De standaard is in beheer bij de internationale organisatie IETF. Het standaardisatieproces van IETF is voldoende open. IETF is beheerorganisatie van meerdere standaarden die op de lijst met open standaarden staan waar dit ook getoetst 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.

2. Toegevoegde waarde
De interoperabiliteitswinst en andere voordelen van adoptie van de standaard wegen overheidsbreed en maatschappelijk op tegen de kosten, de risico's en nadelen. Voor elk van de te onderscheiden stakeholders

(overheid, bedrijven en burgers) afzonderlijk zouden de baten voor de informatievoorziening en de bedrijfsvoering op moeten wegen tegen de kosten. Verder moeten de risico's aan overheidsbrede adoptie van de standaard (beveiliging, privacy) acceptabel zijn.

De kosten voor certificaten zijn duur, ongeveer 1500 euro per certificaat. De voordelen wegen op tegen de kosten als een organisatie het van het grootste belang acht alle mogelijke veiligheid 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 het grootste belang is, of waarbij de vertrouwelijkheid van de mail hoog is. In dat geval is er altijd een positieve businesscase.

Een mogelijk beveiligingsrisico is dat zodra de sleutel gekraakt is of op straat is komen te liggen ook de gehele historie is te achterhalen. In de afweging om S/MIME wel of niet te gebruiken is het toch verstandig ondanks dit risico de standaard te gebruiken.

3. Draagvlak
Aanbieders en gebruikers moeten voldoende ervaring hebben met de implementatie en het gebruik van de standaard.

Er is nog onvoldoende duidelijkheid over het gebruik van de standaard binnen de overheid. Organisaties die S/MIME lijken te gebruiken zijn SURFnet, MinAZ, ISOC, KPN, Measuremail, Ericsson, Google, Swisscom, DENIC (Duitse SIDN), Symantec en het Duitse Bundesambt. Bevestiging dat deze organisaties S/MIME ook daadwerkelijk gebruiken is niet bekend. Experts van MinAZ en SURFnet zullen in ieder geval benaderd moeten worden om te bepalen wat hun ervaring is met de standaard.

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.

4. Opname bevordert adoptie
De opname op de lijst moet een geschikt middel zijn om de adoptie van de standaard te bevorderen.

Er bestaat onvoldoende bekendheid van de standaard binnen de overheid, waardoor men niet weet in welke gevallen deze standaard van toegevoegde waarde is. In het geval van sterke beveiliging van mailverkeer moet deze bewustwording toenemen, vandaar dat de status 'aanbevolen' op de lijst met open standaarden een geschikt middel is om de adoptie van de standaard te bevorderen.

<u>Conclusie</u>
Er zijn op voorhand geen struikelblokken te verwachten voor het open standaardisatieproces, de toegevoegde waarde en opname bevordert adoptie. Met name het draagvlak is nog onvoldoende duidelijk, het is namelijk niet duidelijk welke overheden de standaard gebruiken of de aanmelding willen ondersteunen. Dit moet uitgezocht worden tijdens de procedure.

5. Samenhang

Het Forum Standaardisatie wil weten of de aangemelde standaard samenhangt met standaarden die reeds op de lijst zijn opgenomen, of standaarden die voor toetsing in aanmerking komen. Uit de intake moet duidelijk worden of dit gevolgen heeft voor de toetsing en eventuele opname van de aangemelde standaard.

1. *Bestaat er samenhang tussen de aangemelde standaard en de verplichte ('pas-toe-of-leg-uit') standaarden die reeds op de lijst zijn opgenomen en wat betekent dit voor de toetsing en eventuele opname van de standaard?*
   Ja, de standaarden SPF, DKIM, STARTTLS en DANE zijn ook encryptiestandaarden. De reikwijdte van deze standaarden is kleiner, maar S/MIME vergt meer werk en kosten om te implementeren. Om die reden moet goed nagedacht worden of de situatie qua beveiliging om S/MIME vraagt.

2. *Bestaat er samenhang tussen de aangemelde standaard en de aanbevolen standaarden die reeds op de lijst zijn opgenomen en wat betekent dit voor de toetsing en eventuele opname van de standaard?*
   Ja, ook hier staan encryptiestandaarden op. De relatie met de 'pas toe of leg uit'-standaarden is vooral van belang.

3. *Bestaat er samenhang tussen de aangemelde standaard en standaarden die in aanmerking komen voor opname op de lijst en wat betekent dit voor de toetsing van de standaard(en)? (Denk bijvoorbeeld ook aan een gezamenlijke toetsing met (een deel van) deze aanvullende standaarden).*
   Ja, PGP is vergelijkbaar met S/MIME. PGP is lastiger in gebruik en kent minder softwareondersteuning. Toch lijken beide standaarden gebruikt te worden en is de vraag wat de verschillen precies zijn in het gebruik. Het is mogelijk dat ook PGP in aanmerking komt voor opname op de lijst.

6. Sponsorschap

De aanmelding van standaarden voor de lijst van het Forum en het Nationaal Beraad dient ondersteund of gesponsord te worden door overheids- en/of (semi)publieke organisaties die de standaard reeds in gebruik hebben (of voornemens zijn dit te doen) en die de beoogde opname op de lijsten ondersteunen. Dit draagt bij aan het draagvlak voor de standaard, geeft zicht op de functionele usecase voor de overheid en helpt bovendien om tijdens de toetsing de juiste experts te benaderen.

1. *Welke overheden en/of (semi)publieke organisaties ondersteunen de aanmelding van de standaard?*
   Er zijn nog geen overheden die de aanmelding van de standaard ondersteunen. Tijdens de procedure moet hier meer informatie over worden opgehaald.

2. Hebben deze organisaties de standaard geïmplementeerd?
   (zie ook punt 7 voor een uitwerking)
   Dat is nog onduidelijk. Er zijn wel partijen genoemd die nog bevraagd moeten worden op het daadwerkelijk gebruik van de standaard.

7. Functionele use case

Voor de standaard dient een duidelijke use case beschikbaar te zijn op basis waarvan overheden en/of instellingen uit de (semi) publieke sector kunnen bepalen of de aangemelde standaard voor hen relevant is en wie eventueel moet deelnemen aan de experttoetsing van de standaard.

Als de standaard niet gebruikt wordt dan kan het voorkomen dat er misbruik wordt gemaakt van de identiteit van personen tussen mailservers en cliënten en dat e-mail gelezen of gewijzigd kunnen worden. Dan doet iemand anders zich voor alsof het de persoon is en maakt daar misbruik van. Voor veel organisaties is de beveiliging tussen mailservers voldoende beveiliging, aangezien het potentiele misbruik van de identiteit in tussen de server en de cliënt niet tot grote impact gaat leiden. In de meeste gevallen gaat er dan niets mis. Als echter wel de hoogste beveiliging nodig is, bijvoorbeeld omdat het ter voorbeeld om ambtenaren gaat die met zeer gevoelige informatie te maken krijgen waarbij de identiteit of de vertrouwelijkheid/integriteit van de boodschap absoluut veilig gesteld moet worden, dan is het aan te raden om de standaard te gebruiken. De impact wanneer de identiteit van een dusdanige ambtenaar of de informatie van de e-mail misbruikt wordt kan namelijk grote gevolgen hebben.

Als de standaard wel gebruikt wordt dan is er vanaf de cliënt (bijvoorbeeld een smartphone of een computer) veiligheid gewaarborgd, waardoor de identiteit op een juiste manier gecontroleerd wordt. Kwaadwillenden hebben het hierdoor een stuk lastiger om hier misbruik van te maken. Vooralsnog is alleen bekend dat via het in bezit komen of kraken van de sleutel hier misbruik van gemaakt kan worden.