**Forum Standaardisatie**

Wilhelmina van Pruisenweg 52
2595 AN Den Haag

Postbus 96810
2509 JE Den Haag

www.forumstandaardisatie.nl

# notitie

| | | | |
|---|---|---|---|
| **Aan:** | Forum Standaardisatie | | |
| **Van:** | Bureau Forum Standaardisatie | | |
| **Datum:** | 3 april 2018 | **Versie** | 1.0 |
| **Betreft:** | Overzicht reactie openbare consultatieronde S/MIME 3.2 | | |
| **Bijlagen:** | 1. Reactie VNG IBD<br>2. Reactie DICTU Technologiebureau en DICTU Security Centre<br>3. Reactie SURFnet (1)<br>4. Reactie SURFnet (2) | | |

**Datum**
3 april 2018

# 1. Reactie VNG IBD

Een opmerking die nog niet was meegenomen (vanuit mijn vorige review) maar volgens mij toch wel een belangrijk aandachtspunt is, is het volgende:
Een nadeel is dat als je vanaf het eindgebruikers device de e-mail gaat versleutelen (met de publieke sleutel van de ontvanger), deze e-mail versleuteld op de e-mailserver wordt opgeslagen. Je hebt de privésleutel van de ontvanger nodig om de e-mail weer leesbaar te maken. Als deze privésleutel dus niet (meer) beschikbaar is, is de versleutelde e-mail dus niet meer te lezen. Organisaties moeten hier dus over nadenken hoe deze hier mee om willen gaan. Een kopie of backup heeft als nadeel dat ook andere de beschikking kunnen krijgen over deze privésleutel wat de authenticiteit in gevaar kan brengen. Hoe weet de ontvanger van een digitaal ondertekent bericht dat dit bericht afkomstig is van de afzender met de privésleutel of van een derde die de beschikking heeft over de privésleutel (de kopie) en zich voordoet als de 'oorspronkelijke' afzender!

# 2. Reactie DICTU Technologiebureau en DICTU Security Centre

Hieronder vindt u de reactie van het DICTU Technologiebureau en DICTU SecurityCentre op de consultatie1 van het Forum Standaardisatie over S/MIME 3.2. Onze belangrijkste opmerking heeft betrekking op de genoemde certificaten. Het expertadvies spreekt over de verplichting om PKIoverheid certificaten te gebruiken voor S/MIME. Het is ons niet bekend waar is vastgelegd dat binnen de overheid voor interne en externe communicatie in principe alleen gebruik gemaakt mag worden van PKIoverheid certificaten. Daarnaast zou deze verplichting een uitbreiding zijn van de S/MIME standaard waarin niet gesproken wordt over de te vertrouwen PKI(s). De kosten die nu genoemd worden voor de certificaten zijn aanzienlijk bij grootschalige invoering van S/MIME. Binnen de overheid is het echter ook mogelijk om gebruik te maken van certificaten op de Rijkspas.

Vraag:
*1. Zijn er volgens u aanvullingen of wijzigingen nodig in paragraaf 1.3, 1.5 en 1.6 ('Doorlopen proces', 'Samenstelling expertgroep' en 'Toelichting standaard') bezien vanuit het doel om het Forum Standaardisatie en Overheidsbreed Beleidsoverleg Digitale Overheid te voorzien van een inhoudelijk relevante toelichting?*
Antwoord DICTU:
Nee

Vraag:
*2. Bent u het eens met het door de expertgroep geadviseerde functioneel toepassingsgebied? [paragraaf 2.1 van het expertadvies]*
Antwoord DICTU:
Ja

Vraag:
*3. Bent u het eens met het door de expertgroep geadviseerde organisatorische werkingsgebied? [paragraaf 2.2 van het expertadvies]*
Antwoord DICTU:
Ja, waarbij wij het gezien de kosten wel wenselijk vinden dit op de lijst met aanbevolen standaarden te houden en niet op de lijst met verplichte standaarden te zetten. Door het als aanbevolen standaard te hebben, kan S/MIME ingevoerd worden voor bepaalde gebruikers, maar hoeft dit niet voor alle gebruikers geïmplementeerd te worden. Dit staat ook in het expertadvies beschreven in paragraaf 3.1.3.1.

Vraag:
*4. Bent u het eens met de constateringen en conclusies van de expertgroep inzake de toegevoegde waarde? [paragraaf 3.1 van het expertadvies]*
Antwoord DICTU:

Nee, we zijn het niet eens met paragraaf 3.1.3.1 waar gesproken wordt over de kosten voor certificaten en de genoemde afspraak dat voor interne en externe communicatie in principe alleen gebruik gemaakt mag worden van PKIoverheid certificaten. Het is ons niet bekend waar is vastgelegd dat binnen de overheid voor interne en externe communicatie in principe alleen gebruik gemaakt mag worden van PKIoverheid certificaten. Een autoratieve referentie zou hier op zijn plaats zijn. Indien die referentie ontbreekt zou in de toekomst PKIoverheid wellicht in een

ander voorstel als standaard opgenomen kunnen worden voor bijvoorbeeld externe communicatie. Bovendien wordt in de S/MIME standaard niet gesproken over de PKI(s) die gebruikt mag/mogen worden.

Toevoeging van de eis voor PKIoverheid certificaten zou een uitbreiding zijn op de standaard. Wij vinden dat het Forum Standaardisatie m.b.t. S/MIME zich moet beperken tot de standaard en hierin geen uitspraken moet doen over de trust. Zeker voor intern gebruik binnen de overheid vinden wij dat bepalen van welke PKI gebruik gemaakt wordt is voorbehouden aan de betrokken organisatie(s) zelf en dat dit niet vastgelegd zou moeten worden door het Forum Standaardisatie. Zo bevat de Rijkspas een authenticatiecertificaat dat binnen S/MIME hiervoor gebruikt zou kunnen worden en zou de Rijkspas daarnaast gemakkelijk voorzien kunnen worden van certificaten voor ondertekening (onloochenbaarheid) en encryptie tegen lagere kosten dan genoemd in het Expertadvies. In geval van een Rijkspas certificaat voor ondertekening zou het niet gaan om een gekwalificeerd elektronische handtekening certificaat, maar wel om een geavanceerde elektronische handtekening die voor veel gevallen voldoende zekerheid biedt over de authenticiteit van afzender, integriteit van het bericht en de onloochenbaarheid daarvan.

In paragraaf 3.1.2.3 wordt daarnaast gerefereerd aan OpenPGP als een vergelijkbare maar niet-concurrerende standaard. Het Expertadvies noemt dat naast S/MIME ook OpenPGP toegevoegd zou kunnen worden aan de lijst met aanbevolen standaarden. Omdat OpenPGP en S/MIME niet samenwerken komt dit de interoperabiliteit niet ten goede. Als het ene ministerie S/MIME zou invoeren en het andere OpenPGP kunnen deze ministeries niet via beveiligde en ondertekende email communiceren. Aangezien het bevorderen van interoperabiliteit één van de doelstellingen is van het Forum Standaardisatie lijkt het ons niet wenselijk beide standaarden (op termijn) aan de lijst toe te voegen.

Vraag:
*5. Bent u het eens met de constateringen en conclusies van de expertgroep inzake het open standaardisatieproces? [paragraaf 3.2 van het expertadvies]* "
Antwoord:
Ja

Vraag:
*6. Bent u het eens met de constateringen en conclusies van de expertgroep inzake het draagvlak? [paragraaf 3.3 van het expertadvies]*
Antwoord:
Ja

Vraag:
*7. Bent u het eens met de constateringen en conclusies van de expertgroep inzake de bevordering van de adoptie door opname op de lijst? [paragraaf 3.4 van het expertadvies]*
Antwoord:
Ja, wat betreft dat een verplichting niet aan de orde is. Wel willen we opmerken dat het naast elkaar laten bestaan van S/MIME en OpenPGP de interoperabiliteit niet ten goede komt omdat de standaarden niet onderling compatibel zijn.

Vraag:
*8. Bent u het eens met het advies van de expertgroep aan het Forum Standaardisatie om S/MIME 3.2 op de lijst aanbevolen standaarden te plaatsen? [Advies aan het Forum]*
Antwoord:
Ja

Vraag:
*9. Bent u het eens met de adoptie-aanbevelingen van de expertgroep aan het Overheidsbreed Beleidsoverleg Digitale Overheid? [paragraaf 3.5 van het expertadvies]*
Antwoord:
Ja

Vraag:
*10. Wilt u aanvullende informatie of overwegingen meegeven aan het Forum Standaardisatie en Overheidsbreed Beleidsoverleg Digitale Overheid die van invloed zouden kunnen zijn op het besluit om S/MIME 3.2 op de lijst met open standaarden te plaatsen?*
Antwoord:
Het voorschrijven van PKIoverheid certificaten voor alle gebruik van S/MIME binnen de overheid lijkt ons ongewenst gezien de ermee gepaard gaande kosten en buiten het toepassingsgebied van de standaard vallen. We stellen voor dat geen specifieke certificaten genoemd worden.

# 3. Reactie SURFnet (1)

In het Consultatiedocument S/MIME (https://www.forumstandaardisatie.nl/sites/bfs/files/20180223%20Consultatiedocument%20S-MIME.pdf) wordt op bladzijde 6 in paragraaf 3.5 gevraagd een reactie te geven op hoofdstuk 3.5 van het expertadvies. Deze ontbreekt echter. Zie ik wat over het hoofd?

# 4. Reactie SURFnet (2)

Voor het grootste gedeelte zijn we het eens met het expertadvies, maar we denken dat er wat meer uitleg nodig is over de nadelen van s/Mime en het verschil met OpenPGP:

Met de meeste vragen zijn we het dan ook eens, hieronder de vragen waar we het niet helemaal mee eens zijn:

Vraag 1:
Hoofdstuk 1.6 behoeft nog wat verdere uitwerking. Er wordt niet ingegaan op eventuele nadelen van het gebruik van deze standaard, zoals het feit dat certificaten verlopen, en eventuele implementatieproblemen bij het gebruik van meerdere devices. Overigens komt dit wel later in het document aan de orde (hoofdstuk 3).

Verder wordt in het onderdeel waar de raakvlakken met OpenPGP besproken worden gesproken van extra handelingen bij certificaat beheer: OpenPGP gebruikt geen certificaten maar sleutelparen.

Vraag 10:
Het verschil tussen s/mime en OpenPGP wordt niet helemaal duidelijk uit het document. S/MIME is afhankelijk van SSL PKI: je hebt een SSL-certificaat met jouw openbare sleutel en het feit dat het is ondertekend door een certificeringsinstantie (CA) "bewijst" dat het echt jouw sleutel is. PGP daarentegen heeft geen PKI: je controleert of iemands publieke sleutel echt van hem is door hem dat te laten opzeggen terwijl hij zijn paspoort laat zien (key signing party) of je vertrouwt de sleutel omdat veel andere mensen deze check al hebben gedaan en die zijn sleutel hebben ondertekend.