



Forum Standaardisatie

**Consultatiedocument S/MIME voor digitale  
ondertekening**

Datum 5 augustus 2018

Colofon

Projectnaam	Consultatiedocument S/MIME voor digitale ondertekening
Versienummer	1.0
Organisatie	Forum Standaardisatie

## Inhoud

<b>Colofon</b> .....	<b>1</b>
<b>Inhoud</b> .....	<b>2</b>
<b>1 Inleiding</b> .....	<b>3</b>
1.1 <i>Doel</i> .....	3
1.2 <i>Achtergrond</i> .....	3
1.3 <i>Plaats van de consultatie in het proces</i> .....	3
<b>2 Consultatieprocedure</b> .....	<b>5</b>
2.1 <i>Het expertadvies</i> .....	5
2.2 <i>Vragen aan u</i> .....	5
2.3 <i>Uw reactie</i> .....	5
2.4 <i>Termijn en adres</i> .....	5
<b>3 Vragen</b> .....	<b>6</b>
3.1 <i>Inleiding</i> .....	6
3.2 <i>Vragen over het advies</i> .....	6
3.3 <i>Resterende inhoudelijke opmerkingen</i> .....	6

## 1 Inleiding

### 1.1 Doel

Dit document bevat vragen ter beantwoording voor de openbare consultatie op het advies om S/MIME alleen voor digitale ondertekening (en niet voor versleuteling) van berichten op te nemen op de lijst aanbevolen standaarden.

### 1.2 Achtergrond

De Nederlandse overheid streeft naar betrouwbare gegevensuitwisseling door het gebruik van open standaarden en het voorkomen van vendor lock-in. Het adviesrapport "Maak Waar!"<sup>1</sup> en de strategie "Nederland Digitaal"<sup>2</sup> 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.

De *instructie Rijk inzake de aanschaf van ICT-producten en ICT-diensten*<sup>3</sup> verplicht (semi-) overheidsorganisaties om bij aanbestedingen relevante standaarden toe te passen die op de 'pas toe of leg uit' lijst staan. Alleen met zwaarwegende redenen mag een organisatie hiervan afwijken, en moet dan de reden hiervan uitleggen in het jaarverslag.

Het Overheidsbreed Beleidsoverleg Digitale Overheid (hierna OBDO) besluit welke standaarden op deze lijst worden opgenomen. Het OBDO baseert zich hierbij op expertadviezen, openbare consultaties en adviezen van het Forum Standaardisatie.

### 1.3 Plaats van de consultatie in het proces

In de vergadering van 25 april 2018 stemde het Forum Standaardisatie in met het advies tot plaatsing van S/MIME op de lijst aanbevolen standaarden. Voordat dit advies kon worden voorgelegd aan het OBDO verscheen op 14 mei een bericht in de media dat een ernstig veiligheidsprobleem met S/MIME was geconstateerd (zie <https://efail.de/>).

Het Forumadvies S/MIME<sup>4</sup> is daarop teruggelegd aan de indiener en de experts. Daarnaast is het NCSC geconsulteerd over de ernst van het veiligheidsprobleem. Het NCSC adviseert om S/MIME niet meer te gebruiken voor de versleuteling van e-mail berichten. S/MIME kan nog wel veilig worden toegepast voor digitale ondertekening van e-mail berichten.

1 <https://www.rijksoverheid.nl/documenten/rapporten/2017/04/18/rapport-van-de-studiegroep-informatiesamenleving-en-overheid-maak-waar>

2 <https://www.rijksoverheid.nl/documenten/rapporten/2018/06/16/nederlandse-digitaliseringsstrategie>

3 <http://wetten.overheid.nl/BWBR0024717/2008-11-23>

4 <https://www.forumstandaardisatie.nl/sites/bfs/files/FS%20180425.3G%20Forum-advies%20S-MIME%203.2.pdf>

De openbare consultatie heeft als doel te toetsen of er draagvlak is om *S/MIME alleen voor digitale ondertekening van e-mail* (niet voor versleuteling van berichten) op de lijst aanbevolen standaarden te plaatsen. Alle reacties uit de consultatie worden samen met het expertadvies aan het Forum Standaardisatie aangeboden.

## 2 Consultatieprocedure

### 2.1 Het expertadvies

Onderwerp van deze consultatie is het advies om S/MIME *alleen voor digitale ondertekening van e-mail* (niet voor de versleuteling van berichten) op de lijst aanbevolen standaarden te plaatsen.

Documenten die ten grondslag liggen aan dit advies zijn:

- Het oorspronkelijke Forumadvies voor plaatsing van S/MIME op de lijst aanbevolen standaarden, gepubliceerd voordat het veiligheidsprobleem met S/MIME bekend was:  
<https://www.forumstandaardisatie.nl/sites/bfs/files/FS%20180425.3G%20Forum-advies%20S-MIME%203.2.pdf>
- Publicatie van de kwetsbaarheid van S/MIME voor het versleutelen van e-mail berichten: <https://efail.de/>

### 2.2 Vragen aan u

Hoofdstuk 3 van dit consultatiedocument stelt u een aantal vragen over het bovenstaand advies.

### 2.3 Uw reactie

Uw reactie bestaat uit een schriftelijke beantwoording van de vragen zoals gesteld in hoofdstuk 3. U mag adviseren om van het advies af te wijken, mits u dit onderbouwt.

Het Forum Standaardisatie maakt de ontvangen reacties openbaar op de website [www.forumstandaardisatie.nl](http://www.forumstandaardisatie.nl). Als u van mening bent dat uw reactie van (bedrijfs-)vertrouwelijke aard is en als zodanig dient te worden behandeld, dient u ook naast de vertrouwelijke versie ook een openbare versie in te dienen. Alleen de openbare versie zal dan worden gepubliceerd.

### 2.4 Termijn en adres

Uw reactie op de vragen in het voorliggende consultatiedocument kunt u per e-mail sturen naar [info@forumstandaardisatie.nl](mailto:info@forumstandaardisatie.nl) onder vermelding van 'Consultatieprocedure S/MIME'.

Uw reactie dient **uiterlijk 10 september 2018** in het bezit te zijn van het Bureau Forum Standaardisatie. Het Forum Standaardisatie behoudt zich het recht voor om reacties ontvangen na 10 september 2018 niet mee te nemen in de besluitvorming.

## 3 Vragen

### 3.1 Inleiding

Dit hoofdstuk bevat een drietal vragen over het advies om S/MIME alleen voor digitale ondertekening van berichten op de lijst aanbevolen standaarden te plaatsen.

### 3.2 Vragen over het advies

*Vragen:*

1. Bent u het eens met het advies om S/MIME *alleen voor digitale ondertekening van e-mail berichten* op de lijst aanbevolen standaarden te plaatsen?
2. Bent u het eens met het advies om S/MIME *niet aan te bevelen voor de versleuteling van e-mail berichten*?

Indien uw antwoord op vraag 1 of 2 'nee' is, verzoeken wij u dit te onderbouwen.

### 3.3 Resterende inhoudelijke opmerkingen

*Vraag:*

3. 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 *alleen voor digitale ondertekening van e-mail berichten* op de lijst aanbevolen open standaarden te plaatsen?