

Hoe de bij S/MIME ontvangen berichten op ESA worden geverifieerd

Inhoud

[Inleiding](#)

[Hoe de bij S/MIME ontvangen berichten op ESA worden geverifieerd teken](#)

[Versleutelen](#)

[Sign/Encrypt](#)

[drievoudig](#)

[Certificaatverificatie](#)

[Gerelateerde informatie](#)

Inleiding

Dit document beschrijft wat u moet controleren in de e-mailbestanden op Cisco Email Security Appliance (ESA) wanneer berichten worden ontvangen met een geldige Secure/Multifunctionele Internet Mail Uitbreidingen (S/MIME).

Hoe de bij S/MIME ontvangen berichten op ESA worden geverifieerd

S/MIME is een op standaarden gebaseerde methode om beveiligde, geverifieerde e-mailberichten te verzenden en ontvangen. S/MIME gebruikt openbare/particuliere toetsenborden om berichten te versleutelen of te ondertekenen.

- Als het bericht versleuteld is, kan alleen de ontvanger van het bericht het gecodeerde bericht openen.
- Als het bericht is getekend, kan de ontvanger van het bericht de identiteit van de afzender valideren en kan hij er zeker van zijn dat het bericht tijdens het transport niet is gewijzigd.

Met een geldig S/MIME-verzendprofiel dat is ingesteld op de ESA, kunnen berichten worden verstuurd met een van de vier modi:

- Sign.
- Versleutelen
- Sign/Encrypt (Sign. en vervolgens encryptie)
- Triple (teken, encryptie en teken opnieuw)

Evenzo kunnen berichten worden ontvangen van andere zenders die geldige S/MIME certificaten voor het ondertekenen of coderen hebben gebruikt.

Voor de ontvanger zullen ze een e-mailtoepassing moeten gebruiken om de gekoppelde digitale handtekening of encryptie correct te verwerken, weer te geven en te accepteren.

Gemeenschappelijke e-mailtoepassingen die de digitale handtekening of encryptie optie zullen presenteren zijn Microsoft Outlook, Mail (OSX) en Mozilla Thunderbird. Het bericht zelf zal een .p7s (smime.p7s) of .p7m (smime.p7m) bijlage bevatten. Deze bijlagebestanden worden met de bericht-ID (MID) opgenomen in de maillogs.

De weergave van een bijlage met het .p7s-bestand is een vlag die het bericht een digitale handtekening draagt.

De weergave van een bijlage met het .p7m-bestand is een vlag die in het bericht een versleutelde S/MIME-handtekening en -encryptie bevat. De berichtinhoud en de bijlagen zijn ingesloten in een smime.p7m-bestand. Er is een privésleutel nodig die overeenkomt met de openbare sleutel in het bericht om het documentbestand te openen.

Als een e-mailtoepassing geen digitale handtekeningen verwerkt, kan een .p7s van .p7m-bestand als bijlage aan het e-mailbericht verschijnen.

teken

Als het bericht van de verzender werd verstuurd met een S/MIME-verzendprofiel dat was ingesteld voor Sign., op de ontvangende ESA, zou het bij het bekijken van de maillogs voor inkomende berichten een .p7s-attachement betekenen:

```
Fri Dec 5 10:38:12 2014 Info: MID 471 attachment 'smime.p7s'
```

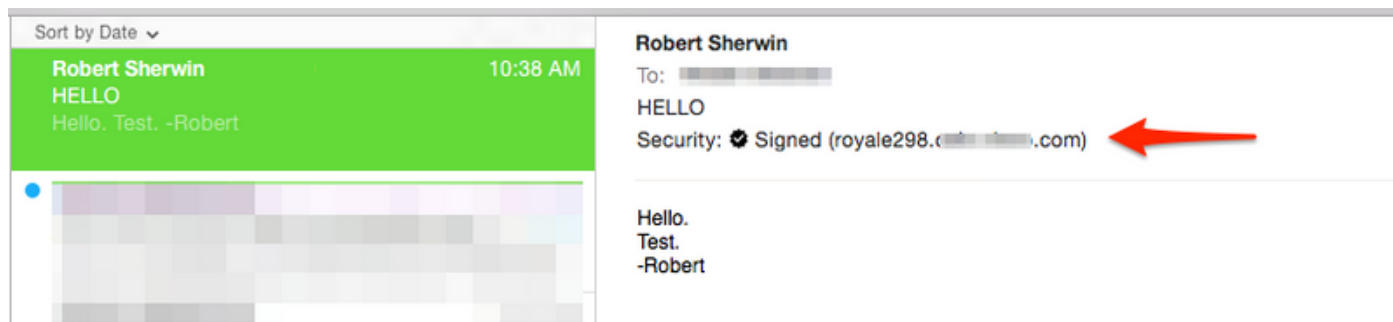
In de ontvangende e-mailapplicatie zou dit op de volgende punten lijken.

Voorbeeld zoals getoond in Outlook 2013 (Windows), merk het teken op van de badge of het certificaatsymbool dat wordt aangegeven:

Robert Sherwin
HELLO
Hello. Test.



 
10:38 AM

Voorbeeld zoals weergegeven Mail (OSX):



Sort by Date ▾

Robert Sherwin 10:38 AM
HELLO
Hello. Test. -Robert

Robert Sherwin
To: [redacted]
HELLO
Security:  Signed (royale298.com) 

Hello.
Test.
-Robert

Versleutelen

Als het bericht van de afzender met een S/MIME-verzendprofiel werd verzonden dat werd ingesteld op Encrypt, zou op de ontvangende ESA, wanneer u de maillogs voor inkomende berichten bekijkt, een .p7m-bijlage worden aangegeven:

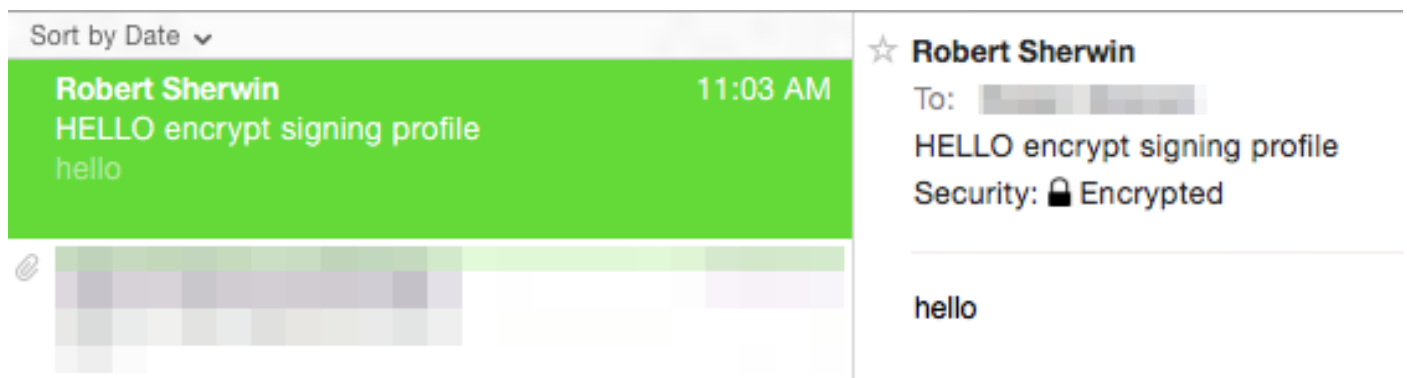
```
Fri Dec 5 11:03:44 2014 Info: MID 474 attachment 'smime.p7m'
```

In de ontvangende e-mailapplicatie zou dit vergelijkbaar zijn met het volgende, merk het hangslot-symbool op dat voor beide voorbeelden is aangegeven.

Voorbeeld zoals in Outlook 2013 (Windows):



Voorbeeld zoals weergegeven Mail (OSX):



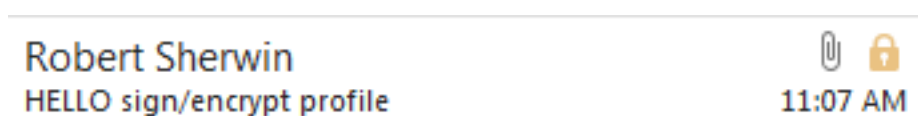
Sign/Encrypt

Als het bericht van de afzender met een S/MIME-verzendprofiel werd verzonden dat werd ingesteld op Sign/Encrypt, op de ontvangende ESA, wanneer u de maillogs voor inkomende berichten bekijkt, zou dit op een .p7m-bijlage wijzen:

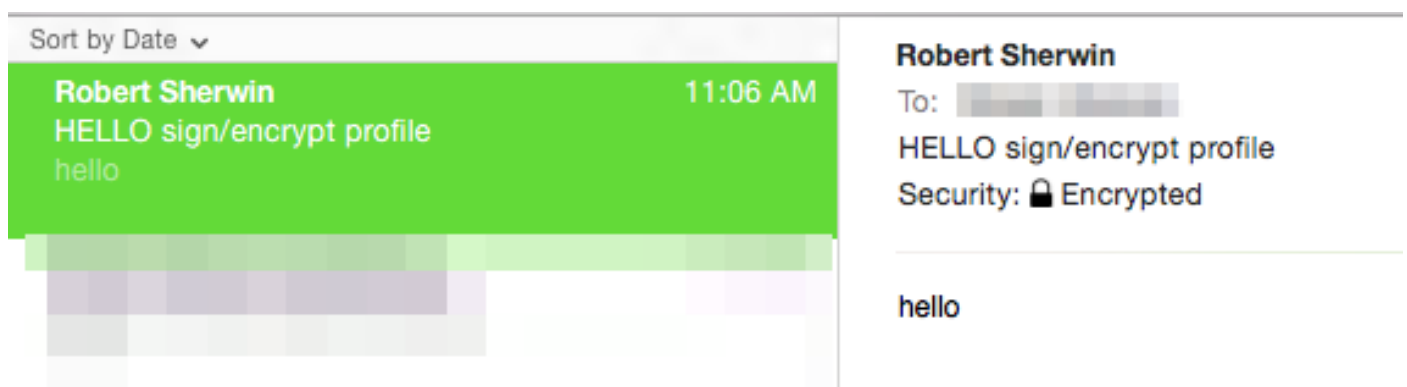
```
Fri Dec 5 11:06:43 2014 Info: MID 475 attachment 'smime.p7m'
```

In de ontvangende e-mailapplicatie zou dit vergelijkbaar zijn met het volgende, merk het aangegeven hangslot-symbool op.

Voorbeeld zoals in Outlook 2013 (Windows):



Voorbeeld zoals weergegeven Mail (OSX):



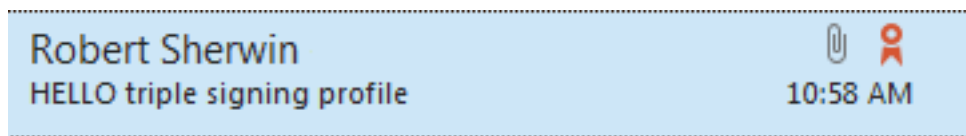
drievoudig

Ten slotte, als het bericht van de verzender werd verstuurd met een S/MIME-profiel dat werd ingesteld op Triple, op de ontvangende ESA, zou het, wanneer het de postlogs voor inkomende berichten bekijkt, zowel een .p7m- als .p7s-bijlage aangeven:

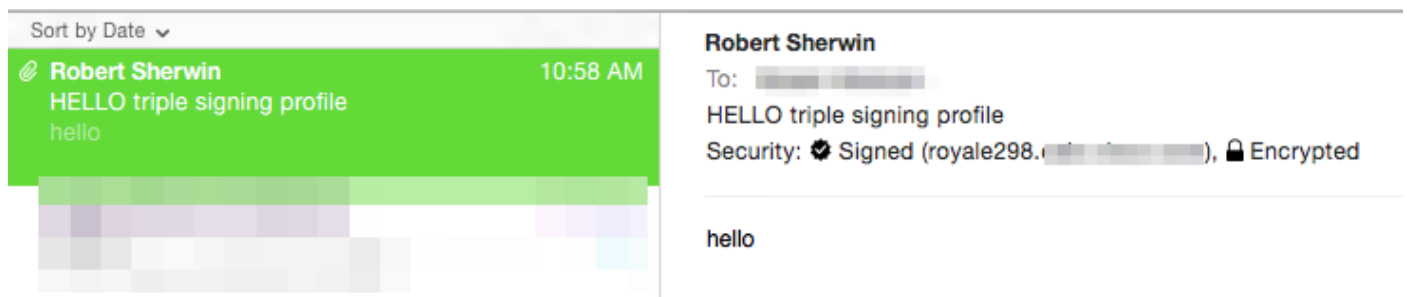
```
Fri Dec 5 10:58:11 2014 Info: MID 473 attachment 'smime.p7m'  
Fri Dec 5 10:58:11 2014 Info: MID 473 attachment 'smime.p7s'
```

In de ontvangende e-mailtoepassing kan dit variëren op basis van de gebruikte e-mailapplicatie.

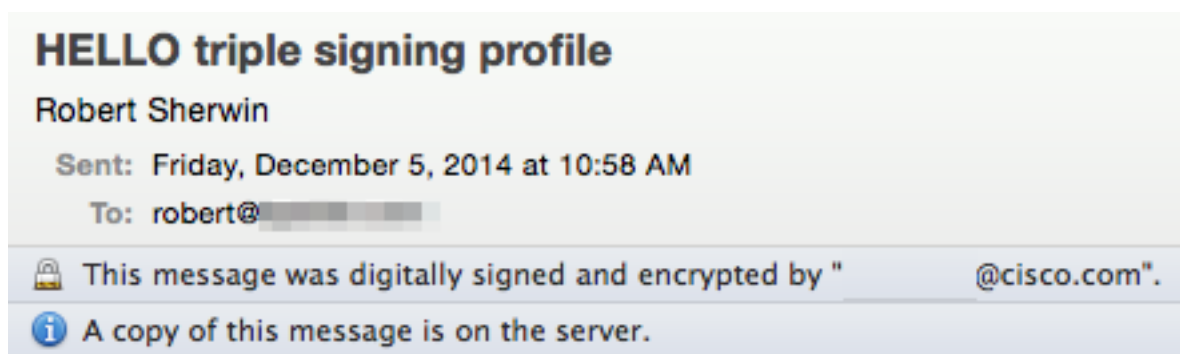
Voorbeeld zoals getoond in Outlook 2013 (Windows), merk het teken op van de badge of het certificaatsymbool dat wordt aangegeven:



Bijvoorbeeld zoals getoond Mail (OSX), merk op dat zowel de badge voor getekend als het hangslot voor encryptie aangegeven is:



Voorbeeld zoals getoond Office 2011 (OSX), merk op dat de hangslot was aangegeven en dat het bericht "Dit bericht werd digitaal ondertekend en versleuteld" was opgenomen:

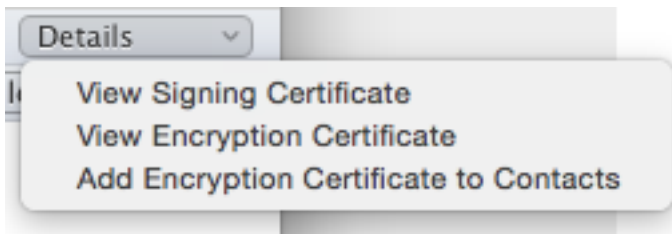


hello

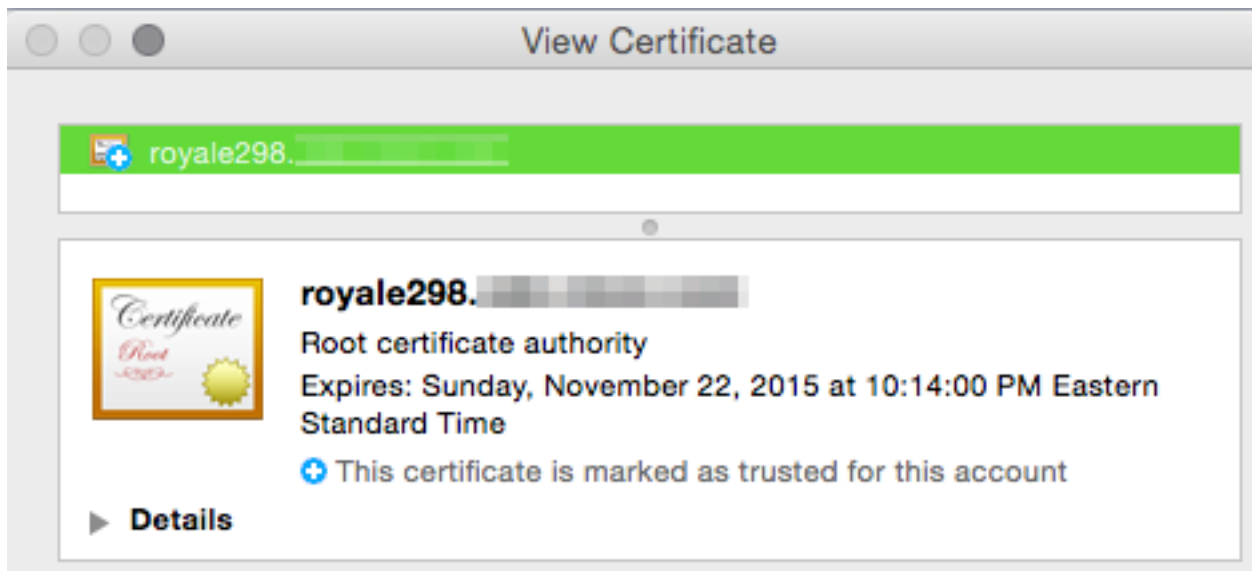
Certificaatverificatie

Gebaseerd op de e-mailtoepassing in gebruik en de voorkeur van de ontvanger, of het veiligheidsbeleid van het bedrijf, zal het bekijken en het accepteren van het certificaat variëren.

In het bovenstaande voorbeeld van drie uitgangen, met Office 2011 (OSX), is er op de ondertekende en gecodeerde berichtenlijn een optie voor het afstempelen van details:



Het **Beeld Signing certificaatcertificaat** selecteren geeft de eigenlijke informatie over het gebarentaal van de ESA weer, die oorspronkelijk werd verzonden van:



Gerelateerde informatie

- [Bestaan van berichten die worden verzonden met S/MIME-verkeersprofiel op ESA](#)
- [Technische ondersteuning en documentatie – Cisco Systems](#)
- [Cisco e-mail security applicatie - gebruikershandleidingen](#)