

Überprüfen von Nachrichten, die mit S/MIME auf ESA empfangen wurden

Inhalt

[Einführung](#)

[Überprüfen von Nachrichten, die mit S/MIME auf ESA empfangen wurden](#)

[Signieren](#)

[Verschlüsseln](#)

[Signieren/Verschlüsseln](#)

[Dreifach](#)

[Zertifikatsüberprüfung](#)

[Zugehörige Informationen](#)

Einführung

Dieses Dokument beschreibt, was in den E-Mail-Protokollen der Cisco E-Mail Security Appliance (ESA) überprüft werden muss, wenn Nachrichten mit einer gültigen S/MIME-Konfiguration (Secure/Multipurpose Internet Mail Extensions) empfangen werden.

Überprüfen von Nachrichten, die mit S/MIME auf ESA empfangen wurden

S/MIME ist eine standardbasierte Methode zum Senden und Empfangen sicherer, verifizierter E-Mail-Nachrichten. S/MIME verwendet ein öffentliches/privates Schlüsselpaar zum Verschlüsseln oder Signieren von Nachrichten.

- Wenn die Nachricht verschlüsselt ist, kann nur der Empfänger der Nachricht die verschlüsselte Nachricht öffnen.
- Wenn die Nachricht signiert ist, kann der Empfänger der Nachricht die Identität des Absenders validieren und sicherstellen, dass die Nachricht während der Übertragung nicht geändert wurde.

Wenn für die ESA ein gültiges S/MIME-Sendeprofil konfiguriert ist, können Nachrichten mit einem von vier Modi gesendet werden:

- Signieren
- Verschlüsseln
- Signieren/Verschlüsseln (Signieren und anschließend verschlüsseln)
- Dreifach (Signieren, Verschlüsseln und erneutes Signieren)

Ebenso können Nachrichten von anderen Absendern empfangen werden, die gültige S/MIME-Zertifikate für Signierung oder Verschlüsselung verwendet haben.

Der Empfänger muss eine E-Mail-Anwendung verwenden, um die zugehörige digitale Signatur oder Verschlüsselung ordnungsgemäß verarbeiten, anzeigen und akzeptieren zu können. Häufig

verwendete E-Mail-Anwendungen, die die digitale Signatur oder Verschlüsselungsoption darstellen, sind Microsoft Outlook, Mail (OSX) und Mozilla Thunderbird. Die Nachricht selbst enthält eine Anlage mit der Erweiterung .p7s (smime.p7s) oder .p7m (smime.p7m). Diese Anhangsdateien werden mit der Nachrichten-ID (MID) in den E-Mail-Protokollen aufgezeichnet.

Die Anzeige eines Anhangs mit der Datei .p7s ist ein Flag, der anzeigt, dass die Nachricht eine digitale Signatur enthält.

Das Aussehen eines Anhangs mit der .p7m-Datei ist ein Flag, dass die Nachricht eine verschlüsselte S/MIME-Signatur und -Verschlüsselung enthält. Der Nachrichteninhalt und die Anhänge werden in einer Datei smime.p7m zusammengefasst. Zum Öffnen der Dokumentdatei wird ein privater Schlüssel benötigt, der mit dem öffentlichen Schlüssel in der Nachricht übereinstimmt.

Wenn eine E-Mail-Anwendung digitale Signaturen nicht behandelt, wird eine .p7s-Datei mit der Erweiterung .p7m möglicherweise als Anhang der E-Mail angezeigt.

Signieren

Wenn die Nachricht vom Absender mit einem S/MIME-Sendeprofil gesendet wurde, das auf Signieren gesetzt war, weist die Empfänger-ESA beim Anzeigen der E-Mail-Protokolle für eingehende Nachrichten auf einen .p7s-Anhang hin:

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

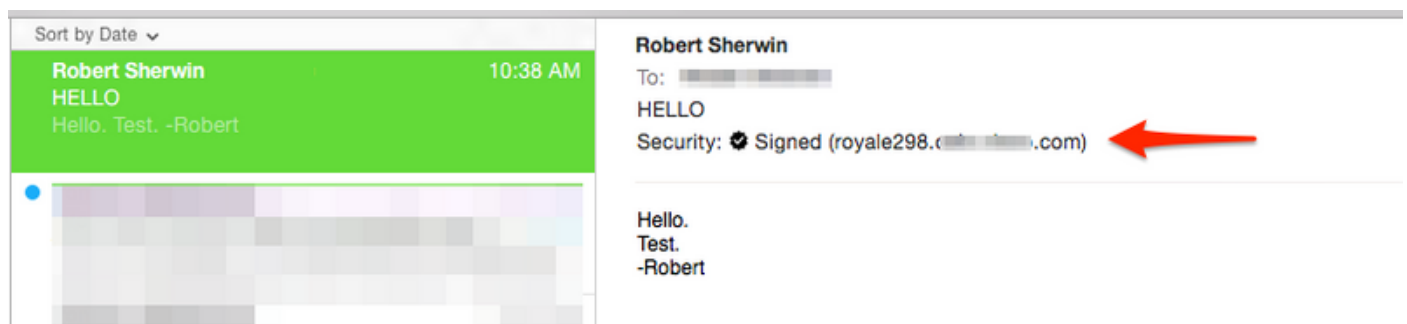
In der E-Mail-Anwendung des Empfängers sieht die Anzeige ähnlich aus wie die folgende.

Wie in Outlook 2013 (Windows) gezeigt, achten Sie auf das angegebene Badge- oder Zertifikatssymbol:

Robert Sherwin
HELLO
Hello. Test.



 
10:38 AM

Beispiel wie gezeigt Mail (OSX):



Sort by Date ▾

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

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

Hello.
Test.
-Robert

Verschlüsseln

Wenn die Nachricht vom Absender mit einem S/MIME-Sendeprofil gesendet wurde, das auf "Encrypt" (Verschlüsseln) gesetzt ist, weist die Empfänger-ESA beim Anzeigen der E-Mail-Protokolle für eingehende Nachrichten auf eine 0,60 m-Anlage hin:

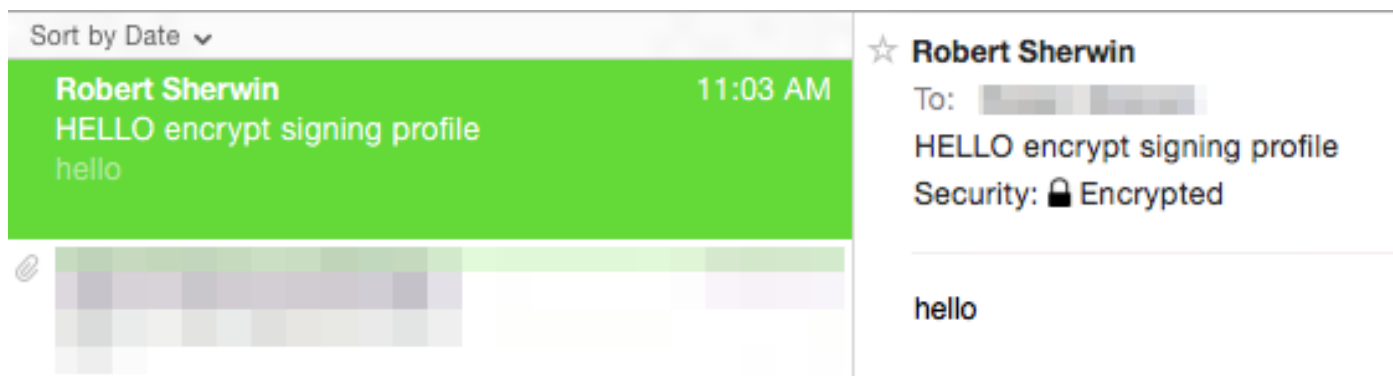
Fri Dec 5 11:03:44 2014 Info: MID 474 attachment 'smime.p7m'

In der E-Mail-Anwendung des Empfängers sieht die Anzeige ähnlich wie die folgende aus. Beachten Sie das für beide Beispiele angezeigte Vorhängeschloss-Symbol.

Beispiel wie in Outlook 2013 (Windows) gezeigt:



Beispiel wie gezeigt Mail (OSX):



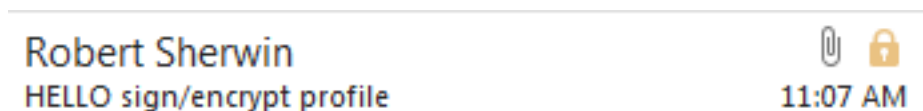
Signieren/Verschlüsseln

Wenn die Nachricht vom Absender mit einem S/MIME-Sendeprofil gesendet wurde, das auf "Signieren/Verschlüsseln" gesetzt ist, weist die Empfänger-ESA beim Anzeigen der E-Mail-Protokolle für eingehende Nachrichten auf eine .p7m-Anlage hin:

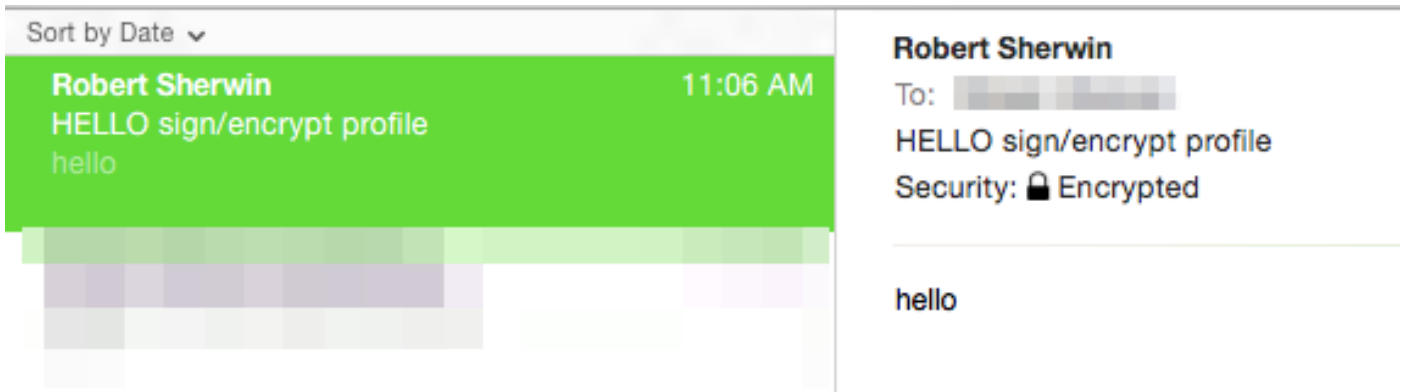
Fri Dec 5 11:06:43 2014 Info: MID 475 attachment 'smime.p7m'

In der E-Mail-Anwendung des Empfängers würde dies ähnlich wie folgt aussehen, beachten Sie das angezeigte Vorhängeschloss-Symbol.

Beispiel wie in Outlook 2013 (Windows) gezeigt:



Beispiel wie gezeigt Mail (OSX):



Dreifach

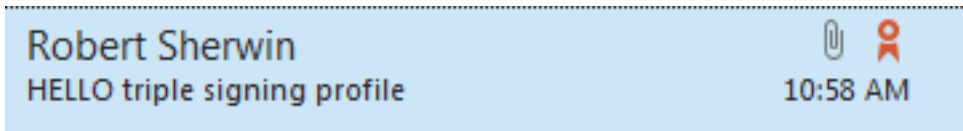
Wenn die Nachricht schließlich vom Absender mit einem S/MIME-Sendeprofil gesendet wurde, das auf Triple festgelegt war, weist die Empfänger-ESA beim Anzeigen der E-Mail-Protokolle für eingehende Nachrichten sowohl einen Anhang mit einem S/MIME-Wert als auch einen Anhang mit einem p7m- und einem p7s-Wert auf:

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

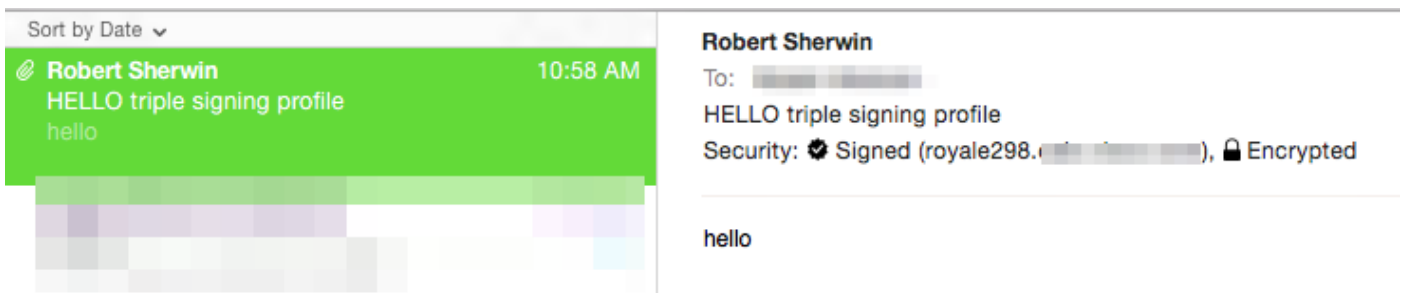
```
Fri Dec 5 10:58:11 2014 Info: MID 473 attachment 'smime.p7s'
```

In der E-Mail-Anwendung des Empfängers kann dies je nach der verwendeten E-Mail-Anwendung variieren.

Wie in Outlook 2013 (Windows) gezeigt, achten Sie auf das angegebene Badge- oder Zertifikatssymbol:



Beachten Sie, dass, wie in der Anzeige "Mail" (OSX) gezeigt, sowohl das Badge für signierte Nachrichten als auch das Vorhängeschloss für die Verschlüsselung angezeigt wird:




Beachten Sie, wie in Office 2011 (OSX) gezeigt, das Vorhängeschloss und die Meldung "Diese Nachricht wurde digital signiert und verschlüsselt" enthalten:


HELLO triple signing profile

Robert Sherwin

Sent: Friday, December 5, 2014 at 10:58 AM

To: robert@

 This message was digitally signed and encrypted by " @cisco.com".

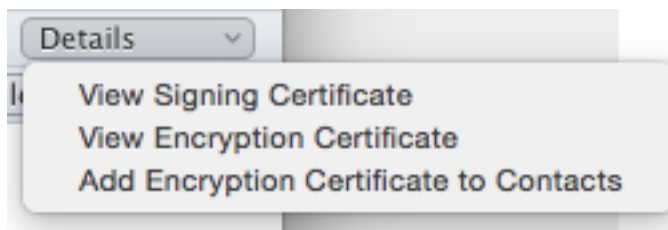
 A copy of this message is on the server.

hello

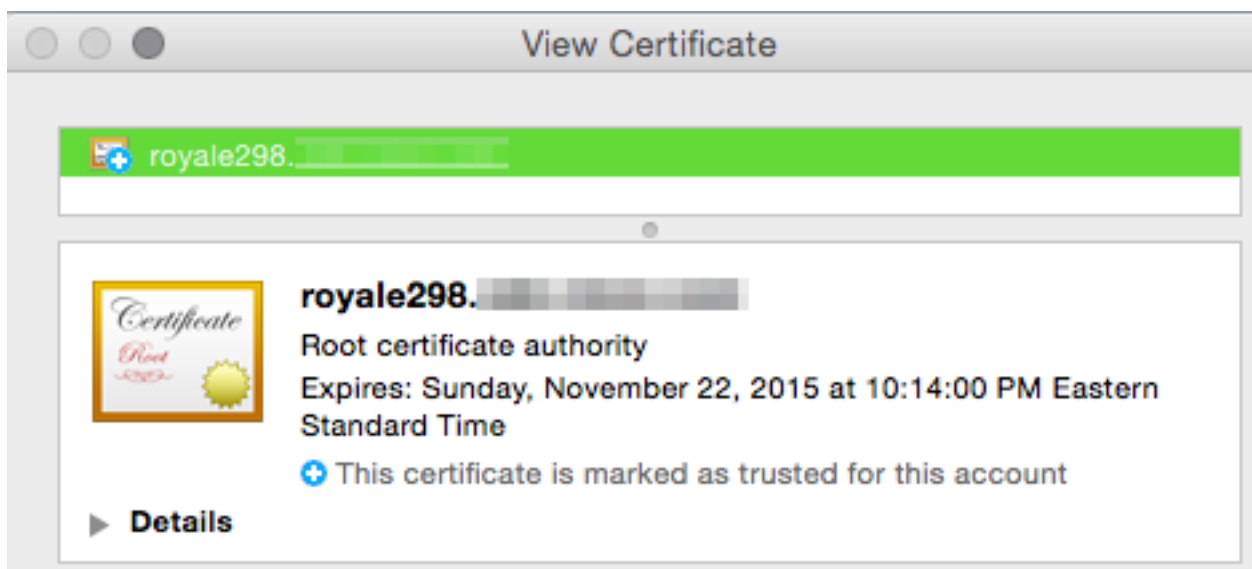
Zertifikatsüberprüfung

Je nach der verwendeten E-Mail-Anwendung und den Präferenzen des Empfängers oder den Sicherheitsrichtlinien des Unternehmens variiert das Anzeigen und Akzeptieren des Zertifikats.

Für das drei obige Beispiel mit Office 2011 (OSX) gibt es auf der signierten und verschlüsselten Nachrichtenzeile eine Dropdown-Option für Details:



Durch die Auswahl des **Signaturzertifikats anzeigen** werden die tatsächlichen Signaturzertifikatsinformationen der ESA angezeigt, von der das ursprünglich gesendet wurde:



Zugehörige Informationen

- [Überprüfen von Nachrichten, die mit S/MIME-Sendeprofil auf der ESA gesendet wurden](#)
- [Technischer Support und Dokumentation - Cisco Systems](#)
- [Cisco Email Security Appliance - Benutzerhandbücher](#)