Come verificare i messaggi ricevuti con S/MIME su ESA

Sommario

[Introduzione](#)
[Come verificare i messaggi ricevuti con S/MIME su ESA](#)
[Firma](#)
[Crittografia](#)
[Firma/Crittografa](#)
[Triplo](#)
[Verifica certificato](#)
[Informazioni correlate](#)

Introduzione

In questo documento viene descritto cosa verificare nei log di posta di Cisco Email Security Appliance (ESA) quando si ricevono messaggi con una configurazione S/MIME (Secure/Multipurpose Internet Mail Extensions) valida.

Come verificare i messaggi ricevuti con S/MIME su ESA

S/MIME è un metodo basato su standard per l'invio e la ricezione di messaggi e-mail sicuri e verificati. S/MIME utilizza una coppia di chiavi pubblica/privata per crittografare o firmare i messaggi.

·Se il messaggio è crittografato, solo il destinatario può aprirlo.
·Se il messaggio è firmato, il destinatario può convalidare l'identità del mittente e assicurarsi che il messaggio non sia stato alterato durante la trasmissione.

Se sull'ESA è stato configurato un profilo di invio S/MIME valido, i messaggi possono essere inviati in una delle quattro modalità descritte di seguito.

· Firma
· Crittografia
· Firma/Crittografa (firma e quindi crittografa)
· Triplo (firma, crittografa e quindi firma di nuovo)

Analogamente, è possibile ricevere messaggi da altri mittenti che hanno utilizzato certificati S/MIME validi per la firma o la crittografia.

Il destinatario dovrà utilizzare un'applicazione di posta elettronica per elaborare, visualizzare e accettare correttamente la firma digitale o la crittografia associata. Le applicazioni di posta elettronica più comuni che presentano la firma digitale o l'opzione di crittografia sono Microsoft Outlook, Mail (OSX) e Mozilla Thunderbird. Il messaggio stesso conterrà un allegato .p7s (smime.p7s) o .p7m (smime.p7m). Questi file allegati verranno registrati con l'ID messaggio (MID)

nei log di posta.

L'aspetto di un allegato con il file con estensione p7s è contrassegno che indica che il messaggio contiene una firma digitale.
L'aspetto di un allegato con il file p7m è un contrassegno che indica che il messaggio contiene una firma e una crittografia S/MIME crittografata. Il contenuto e gli allegati del messaggio sono racchiusi in un file smime.p7m. Per aprire il file del documento è necessaria una chiave privata corrispondente alla chiave pubblica nel messaggio.
Se un'applicazione di posta elettronica non gestisce le firme digitali, un file con estensione p7s di tipo p7m può essere visualizzato come allegato al messaggio di posta elettronica.

Firma

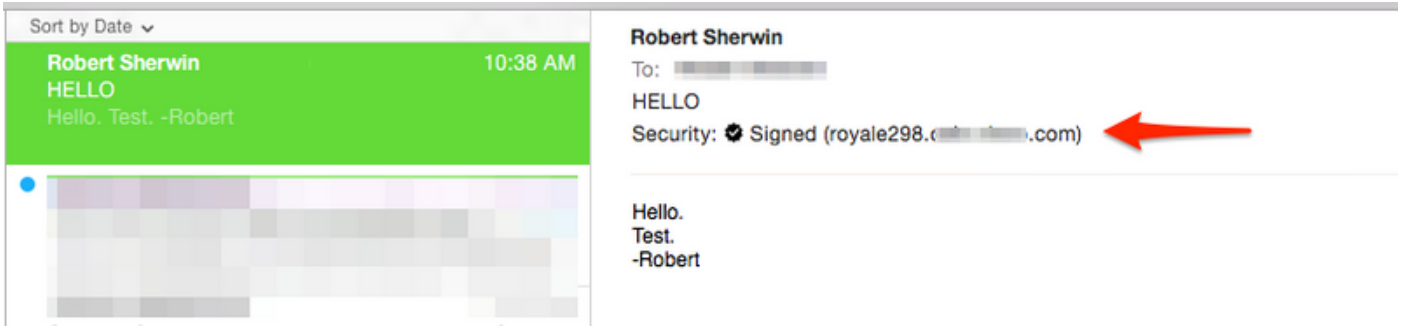
Se il messaggio è stato inviato dal mittente con un profilo di invio S/MIME impostato su Firma, nell'ESA del destinatario, quando si visualizzano i log di posta per i messaggi in arrivo, si indica un allegato .p7s :

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

Nell'applicazione di posta elettronica del destinatario, l'aspetto è simile al seguente.

Esempio come mostrato in Outlook 2013 (Windows), notare il badge o il simbolo del certificato indicato:

Esempio di e-mail (OSX):



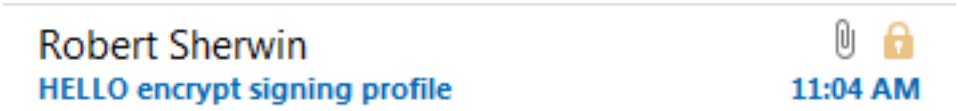
Crittografia

Se il messaggio è stato inviato dal mittente con un profilo di invio S/MIME impostato su Crittografa, nell'ESA del destinatario, quando si visualizzano i log di posta per i messaggi in arrivo, viene indicato un allegato .p7m:

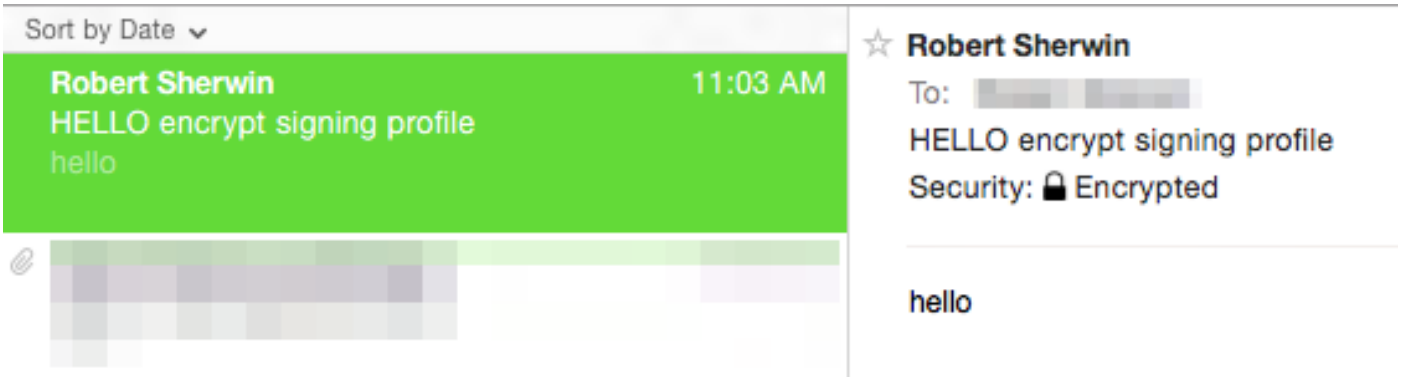
```
Fri Dec 5 11:03:44 2014 Info: MID 474 attachment 'smime.p7m'
```

Nell'applicazione di posta elettronica del destinatario, questo sarebbe simile al seguente, notare il simbolo del lucchetto indicato per entrambi gli esempi.

Esempio come mostrato in Outlook 2013 (Windows):



Esempio di e-mail (OSX):



Firma/Crittografa

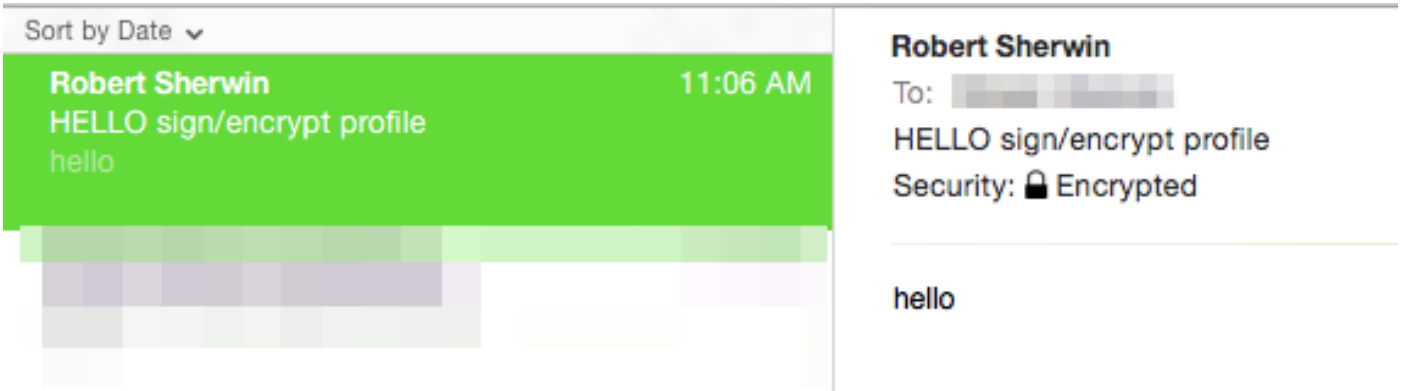
Se il messaggio è stato inviato dal mittente con un profilo di invio S/MIME impostato su Firma/Cripta, sull'ESA del destinatario, quando si visualizzano i log di posta per i messaggi in arrivo, viene indicato un allegato .p7m :

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

Nell'applicazione di posta elettronica del destinatario questo verrebbe visto come segue, notare il simbolo lucchetto indicato.

Esempio come mostrato in Outlook 2013 (Windows):

Esempio di e-mail (OSX):



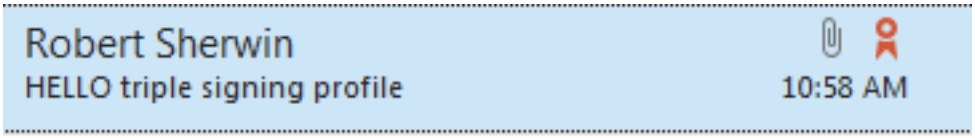
Triplo

Infine, se il messaggio è stato inviato dal mittente con un profilo di invio S/MIME impostato su Tripla, sull'ESA del destinatario, quando si visualizzano i log di posta per i messaggi in arrivo, questo indica sia un allegato p7m che un allegato p7s:

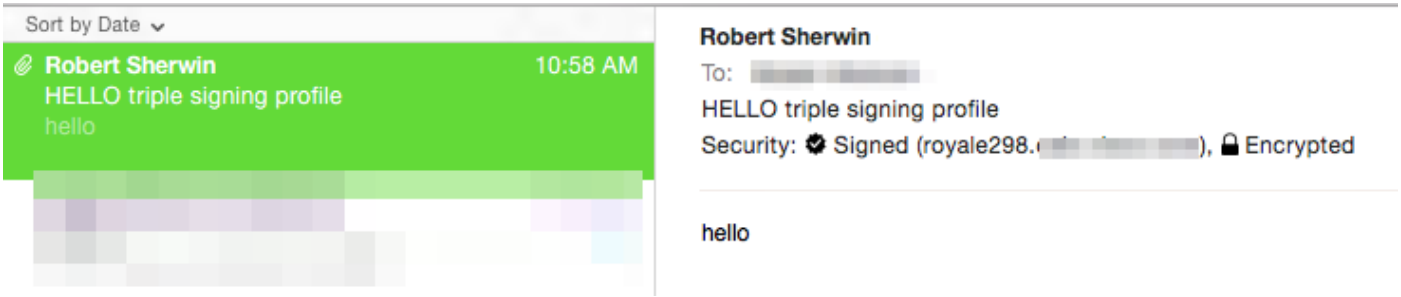
```
Fri Dec 5 10:58:11 2014 Info: MID 473 attachment 'smime.p7m'
Fri Dec 5 10:58:11 2014 Info: MID 473 attachment 'smime.p7s'
```

Nell'applicazione di posta elettronica del destinatario questa impostazione può variare in base all'applicazione di posta elettronica in uso.

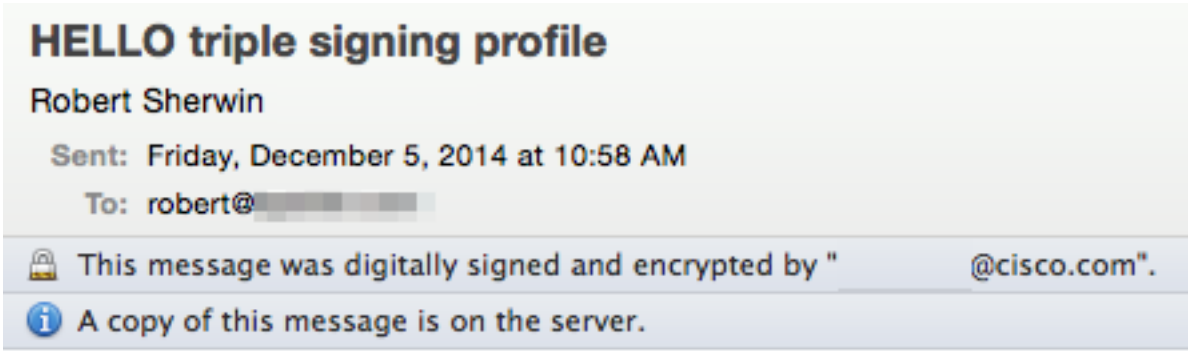
Esempio come mostrato in Outlook 2013 (Windows), notare il badge o il simbolo del certificato indicato:



Esempio come mostrato in Mail (OSX), si noti che viene presentato sia il badge per la firma che il lucchetto per la crittografia:



Esempio come mostrato in Office 2011 (OSX), notare il lucchetto indicato e il messaggio "Messaggio con firma digitale e crittografato" incluso:

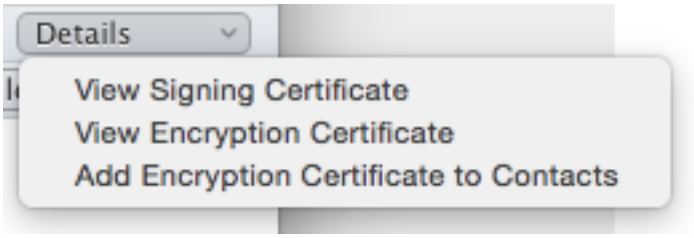



```
hello
```

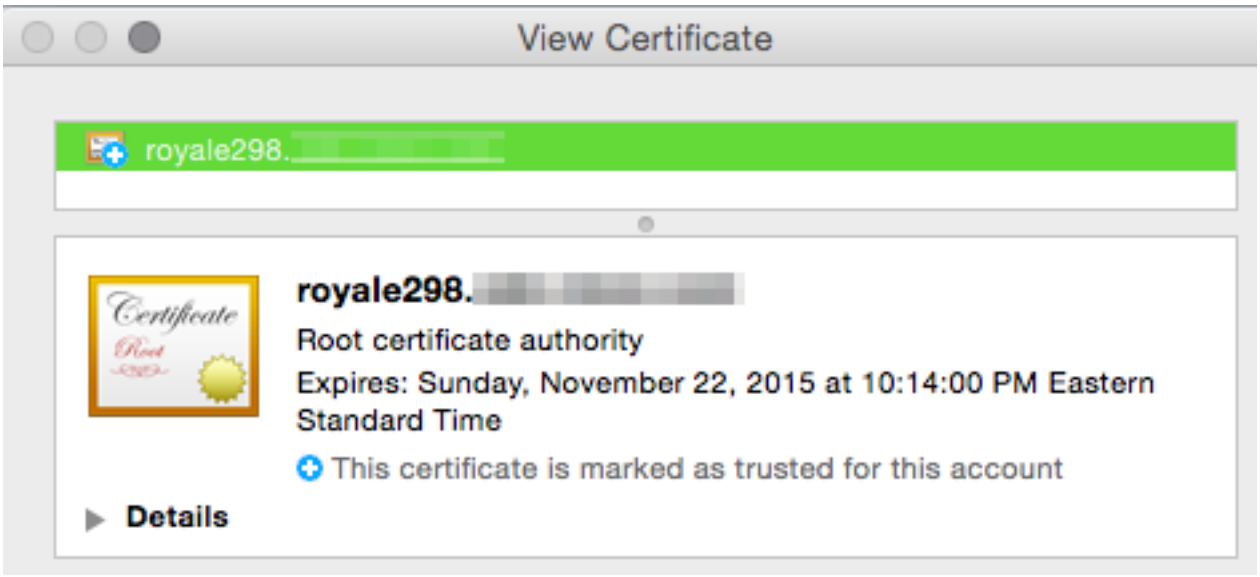
Verifica certificato

La visualizzazione e l'accettazione del certificato variano in base all'applicazione di posta elettronica in uso e alle preferenze del destinatario o ai criteri di sicurezza aziendali.

Per l'esempio triplo precedente, con Office 2011 (OSX), nella riga del messaggio firmato e crittografato è disponibile un'opzione a discesa dei dettagli:



Se si seleziona **Visualizza certificato di firma** vengono visualizzate le informazioni effettive del certificato di firma dell'ESA da cui è stato originariamente inviato il messaggio:



Informazioni correlate

- Come verificare i messaggi inviati con S/MIME Sending Profile su ESA
- Documentazione e supporto tecnico – Cisco Systems
- Cisco Email Security Appliance - Guide per l'utente