Comment vérifier des messages reçus avec S/MIME sur l'ESA

Contenu

Introduction

Ce document décrit quoi vérifier dans la messagerie ouvre une session l'appliance de sécurité du courrier électronique de Cisco (ESA) quand des messages sont reçus avec un valide configuration sécurisent/MIMES (S/MIME).

Comment vérifier des messages reçus avec S/MIME sur l'ESA

S/MIME est une méthode basée sur des standards pour envoyer et recevoir les messages électroniques sécurisés et vérifiés. S/MIME l'utilise paire de clés publique/privée pour chiffrer ou signer des messages.

• Si le message est chiffré, seulement le destinataire du message peut ouvrir le message crypté.
• Si le message est signé, le destinataire du message peut valider l'identité de l'expéditeur et peut être assurément que le message n'a pas été modifié en transit.

Avec un S/MIME valide envoyant le profil configuré sur l'ESA, des messages peuvent être envoyés avec un de quatre modes :

• Signe
• Chiffrez
• Signez/chiffrez (le signe et chiffrent alors)
• Triple (le signe, chiffrent, et puis signent de nouveau)

De même, des messages peuvent être reçus d'autres expéditeurs qui ont utilisé les Certificats valides S/MIME pour la signature ou le cryptage.

Pour le destinataire, ils devront employer une application de messagerie électronique afin de correctement traiter, visualiser, et recevoir la signature numérique ou le cryptage associée. Les applications de messagerie électronique communes qui présenteront la signature numérique ou l'option de chiffrement sont Microsoft Outlook, la messagerie (OSX), et Mozilla Thunderbird. Le message lui-même contiendra une connexion .p7s (smime.p7s) ou de .p7m (smime.p7m). Ces

fichiers de connexion seront enregistrés avec l'ID de message (MID) dans les logs de messagerie.

L'apparence d'une connexion avec le fichier .p7s est indicateur que le message porte une signature numérique.
L'apparence d'une connexion avec le fichier de .p7m est un indicateur que le message porte une signature chiffrée et le cryptage S/MIME. Les contenus du message et les connexions sont enveloppés dans un fichier smime.p7m. Une clé privée appariant la clé publique dans le message est nécessaire pour ouvrir le fichier document.
Si une application de messagerie électronique ne manipule pas des signatures numériques, un .p7s de fichier de .p7m peut apparaître comme connexion au message électronique.

Signe

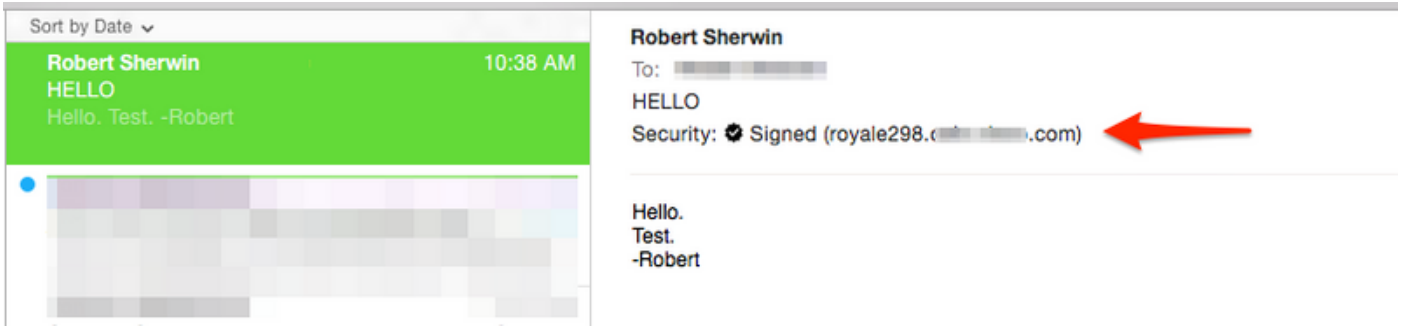
Si le message était envoyé de l'expéditeur avec un S/MIME envoyant le profil qui a été placé pour signer, sur le destinataire ESA, en visualisant la messagerie se connecte pour les messages d'arrivée qu'elle indiquerait un attachement .p7s :

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

Dans l'application d'email du destinataire ce serait semblable vu au suivant.

L'exemple en tant qu'Outlook affiché 2013 (Windows), notent le badge ou délivrent un certificat le symbole indiqué :

Exemple en tant que messagerie affichée (OSX) :



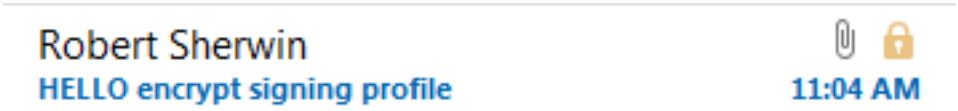
Chiffrez

Si le message était envoyé de l'expéditeur avec un S/MIME envoyant le profil qui a été placé pour chiffrer, sur le destinataire ESA, en visualisant la messagerie se connecte pour les messages d'arrivée qu'elle indiquerait un attachement de .p7m :

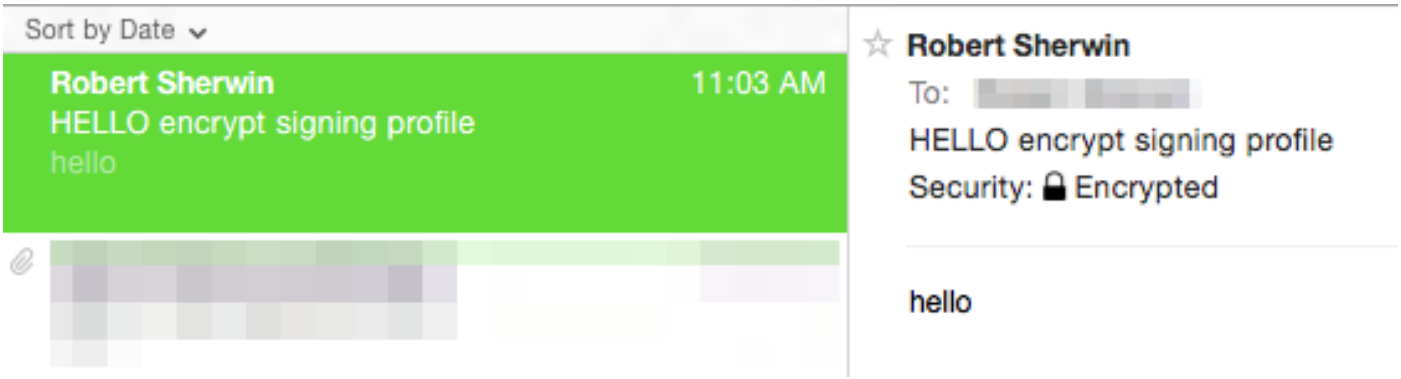
```
Fri Dec 5 11:03:44 2014 Info: MID 474 attachment 'smime.p7m'
```

Dans l'application d'email du destinataire que ce serait semblable vu au suivant, notez le symbole de cadenas indiqué pour les deux exemples.

Exemple en tant qu'Outlook affiché 2013 (Windows) :



Exemple en tant que messagerie affichée (OSX) :



Signez/chiffrez

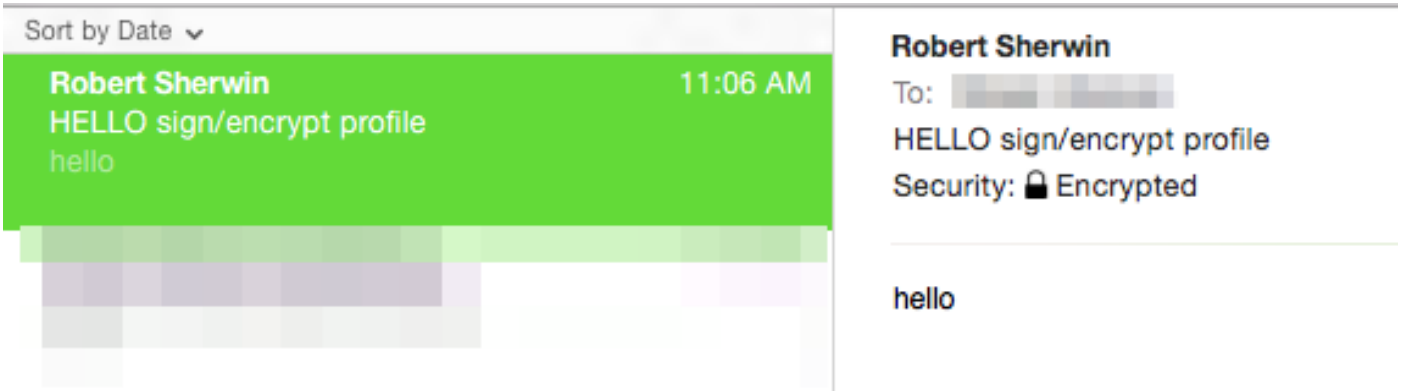
Si le message était envoyé de l'expéditeur avec un S/MIME envoyant le profil qui a été placé pour signer/chiffre, sur le destinataire ESA, en visualisant la messagerie se connecte pour les messages d'arrivée qu'elle indiquerait un attachement de .p7m :

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

Dans l'application d'email du destinataire que ce serait semblable vu au suivant, notez le symbole de cadenas indiqué.

Exemple en tant qu'Outlook affiché 2013 (Windows) :

Exemple en tant que messagerie affichée (OSX) :



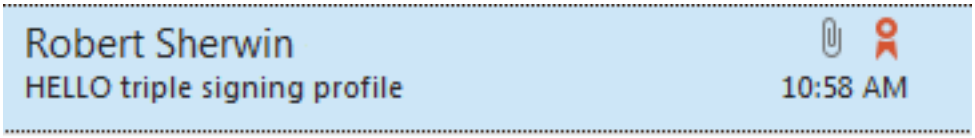
Triple

En conclusion, si le message était envoyé de l'expéditeur avec un S/MIME envoyant le profil qui a été placé pour tripler, sur le destinataire ESA, en visualisant la messagerie se connecte pour les messages d'arrivée l'indiquerait des .p7m et la connexion .p7s :

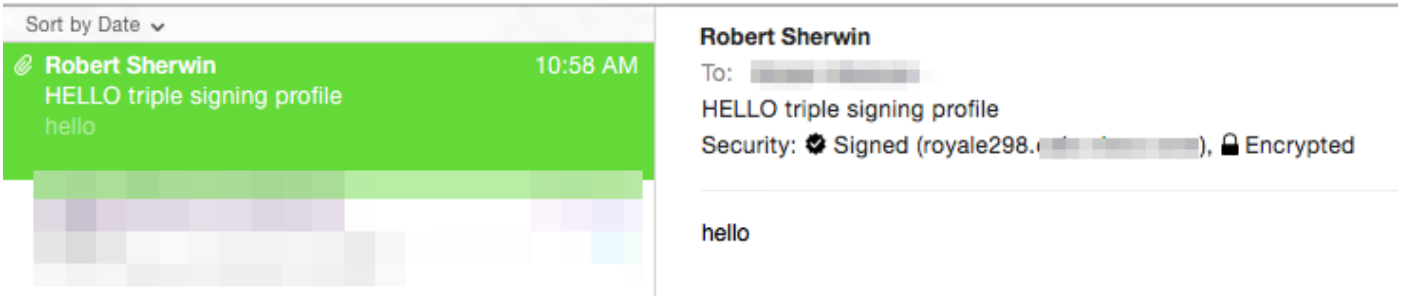
```
Fri Dec 5 10:58:11 2014 Info: MID 473 attachment 'smime.p7m'
Fri Dec 5 10:58:11 2014 Info: MID 473 attachment 'smime.p7s'
```

Dans l'application d'email du destinataire ceci peut varier, basé sur l'application de messagerie électronique en service.

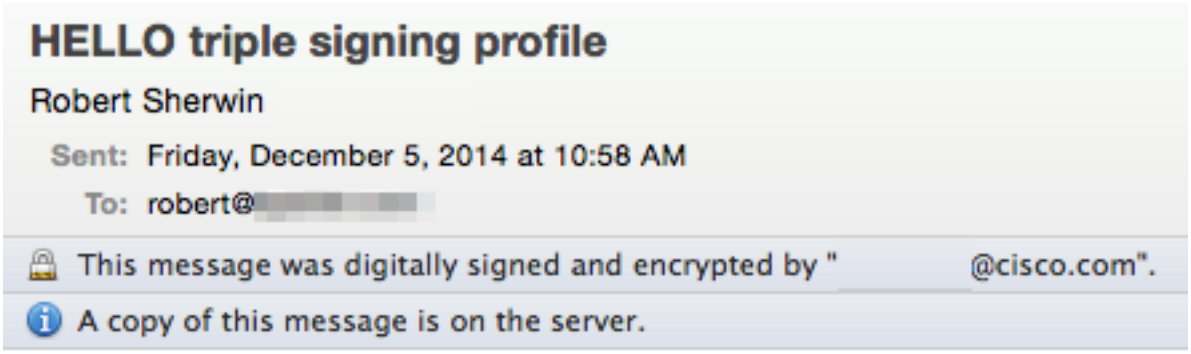
L'exemple en tant qu'Outlook affiché 2013 (Windows), notent le badge ou délivrent un certificat le symbole indiqué :



L'exemple en tant que messagerie affichée (OSX), notent que le badge pour signé est présenté et le cadenas pour le cryptage est indiqué :



L'exemple en tant que bureau affiché 2011 (OSX), notent le cadenas indiqué et le message, « ce message a été digitalement signé et a chiffré » inclus :

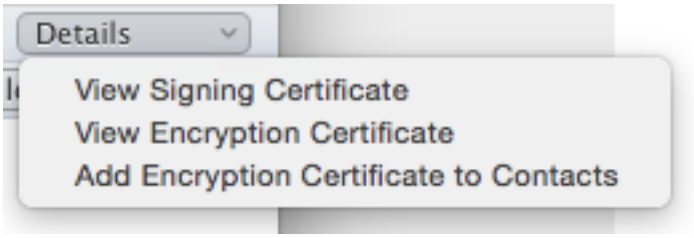



```
hello
```

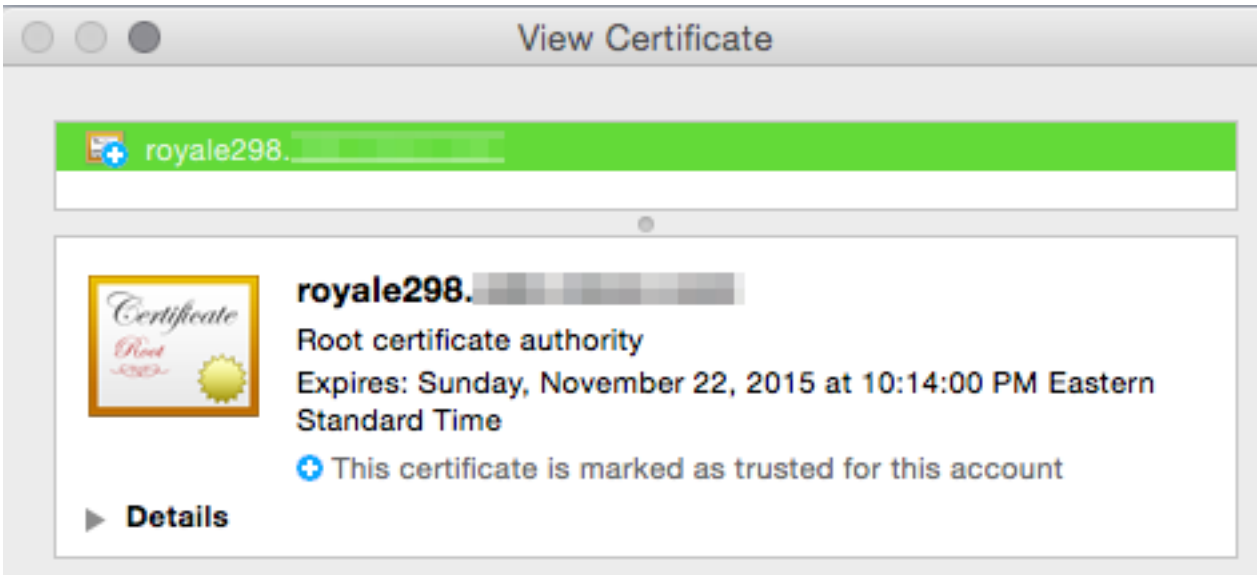
Vérification de certificat

Basé sur l'application de messagerie électronique en service, et la préférence du destinataire, ou des stratégies de sécurité d'entreprise, le visionnement et recevoir du certificat varieront.

Pour l'exemple triple ci-dessus, avec le bureau 2011 (OSX), sur la ligne signée et de message crypté il y a une option déroulante de détails :



Sélectionner le **certificat de signature de vue** présente les informations de signature réelles de certificat de l'ESA que ceci a été initialement envoyé de :



Informations connexes

- Comment vérifier des messages envoyés avec S/MIME envoyant le profil sur l'ESA
- Support et documentation techniques - Cisco Systems
- Appliance de sécurité du courrier électronique de Cisco - Guides utilisateurs