Como verificar as mensagens recebidas com o S/MIME no ESA

Índice

Introdução

Este documento descreve o que verificar no correio entra a ferramenta de segurança do email de Cisco (ESA) quando as mensagens estão recebidas com um válido configuração se fixam/Multipurpose Internet Mail Extension (S/MIME).

Como verificar as mensagens recebidas com o S/MIME no ESA

S/MIME é um método baseado em padrões para enviar e receber mensagens de Email seguros, verificados. S/MIME usa pares do público/chave privada para cifrar ou assinar mensagens.

• Se a mensagem é cifrada, simplesmente o destinatário da mensagem pode abrir o mensagem codificada.
• Se a mensagem é assinada, o destinatário da mensagem pode validar a identidade do remetente e pode ser assegurado que a mensagem não estiver alterada quando no trânsito.

Com um S/MIME válido que envia o perfil configurado no ESA, as mensagens podem ser enviadas com um de quatro modos:

• Sinal
• Cifre
• Assine/cifre (o sinal e cifra então)
• Triplicar-se (o sinal, cifra, e assina então outra vez)

Igualmente, as mensagens podem ser recebidas de outros remetentes que usaram Certificados válidos S/MIME para a assinatura ou a criptografia.

Para o receptor, precisarão de usar um aplicativo de e-mail a fim processar, ver, e aceitar corretamente a assinatura digital ou a criptografia associada. Os aplicativos de e-mail comuns que apresentarão a assinatura digital ou a opção de criptografia são Microsoft outlook, correio (OSX), e Mozilla Thunderbird. A mensagem própria conterá um acessório .p7s (smime.p7s) ou de .p7m (smime.p7m). Estes arquivos do acessório serão gravados com o ID de mensagem

(MEADOS DE) nos logs do correio.

A aparência de um acessório com o arquivo .p7s é bandeira que a mensagem leva uma assinatura digital.
A aparência de um acessório com o arquivo de .p7m é uma bandeira que a mensagem leva uma assinatura cifrada e a criptografia S/MIME. Os conteúdos de mensagem e os acessórios são envolvidos em um arquivo smime.p7m. Uma chave privada que combina a chave pública na mensagem é precisada de abrir o arquivo de documento.
Se um aplicativo de e-mail não segura assinaturas digital, um .p7s do arquivo de .p7m pode aparecer como um acessório ao mensagem de Email.

Sinal

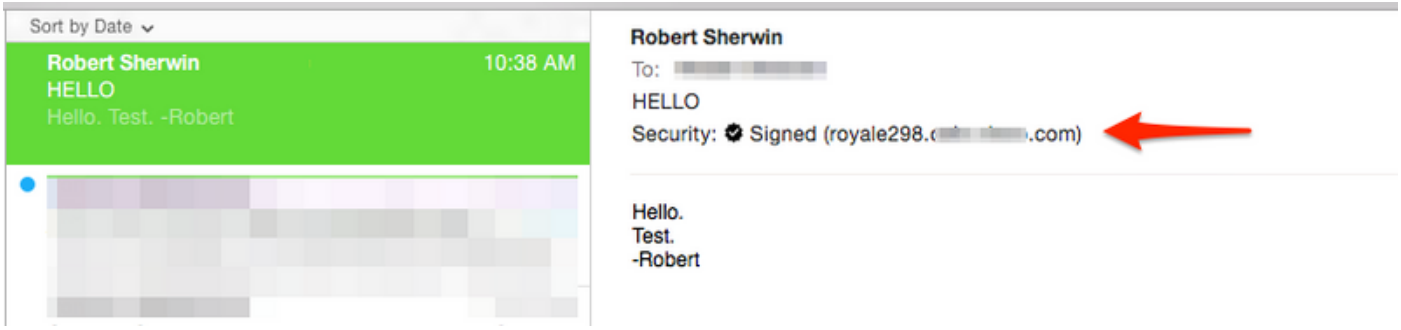
Se a mensagem foi enviada do remetente com um S/MIME que envia o perfil que esteve ajustado para assinar, no receptor ESA, quando ver o correio registrar para mensagens que de entrada indicaria um attachement .p7s:

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

No aplicativo de e-mail destinatário este seria similar visto ao seguinte.

A probabilidade 2013 do exemplo como mostrado (Windows), observa o símbolo do crachá ou do certificado indicado:

Correio do exemplo como mostrado (OSX):



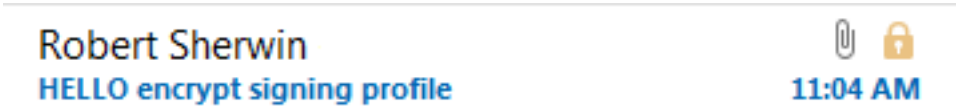
Cifre

Se a mensagem foi enviada do remetente com um S/MIME que envia o perfil que esteve ajustado para cifrar, no receptor ESA, quando ver o correio registrar para mensagens que de entrada indicaria um attachement de .p7m:

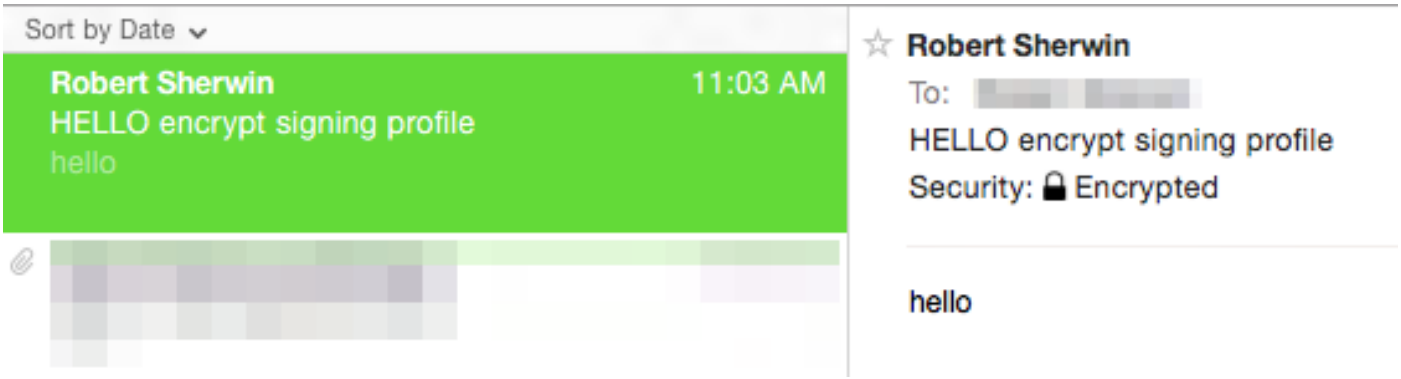
```
Fri Dec 5 11:03:44 2014 Info: MID 474 attachment 'smime.p7m'
```

No aplicativo de e-mail que destinatário este seria similar visto ao seguinte, observe o símbolo do cadeado indicado para ambos os exemplos.

Probabilidade 2013 do exemplo como mostrado (Windows):



Correio do exemplo como mostrado (OSX):



Assine/cifre

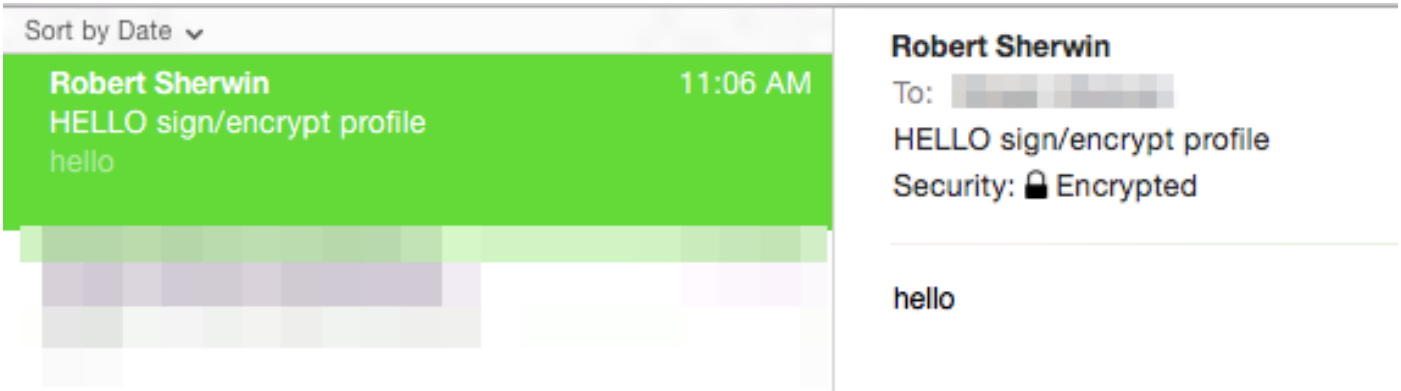
Se a mensagem foi enviada do remetente com um S/MIME que envia o perfil que foi ajustado para assinar/cifrado, no receptor ESA, quando ver o correio registra para mensagens que de entrada indicaria um attachement de .p7m:

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

No aplicativo de e-mail que destinatário este seria similar visto ao seguinte, observe o símbolo do cadeado indicado.

Probabilidade 2013 do exemplo como mostrado (Windows):

Correio do exemplo como mostrado (OSX):



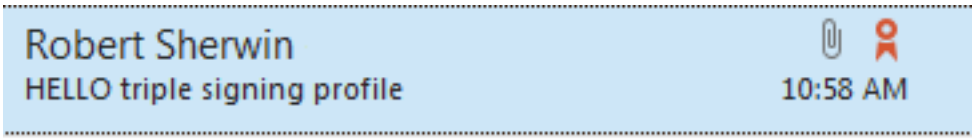
Triplicar-se

Finalmente, se a mensagem foi enviada do remetente com um S/MIME que envia o perfil que esteve ajustado para triplicar, no receptor ESA, quando ver o correio o registra para mensagens de entrada indicaria uns .p7m e o acessório .p7s:

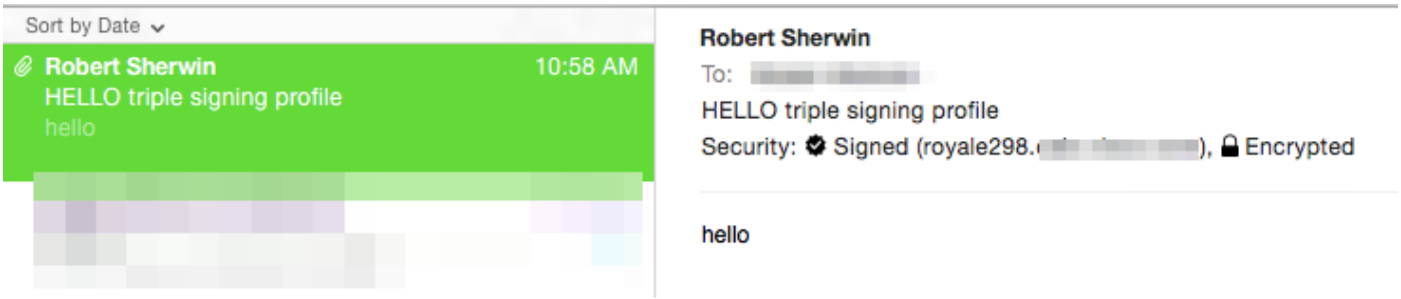
```
Fri Dec 5 10:58:11 2014 Info: MID 473 attachment 'smime.p7m'
Fri Dec 5 10:58:11 2014 Info: MID 473 attachment 'smime.p7s'
```

No aplicativo de e-mail destinatário isto pode variar, com base no aplicativo de e-mail no uso.

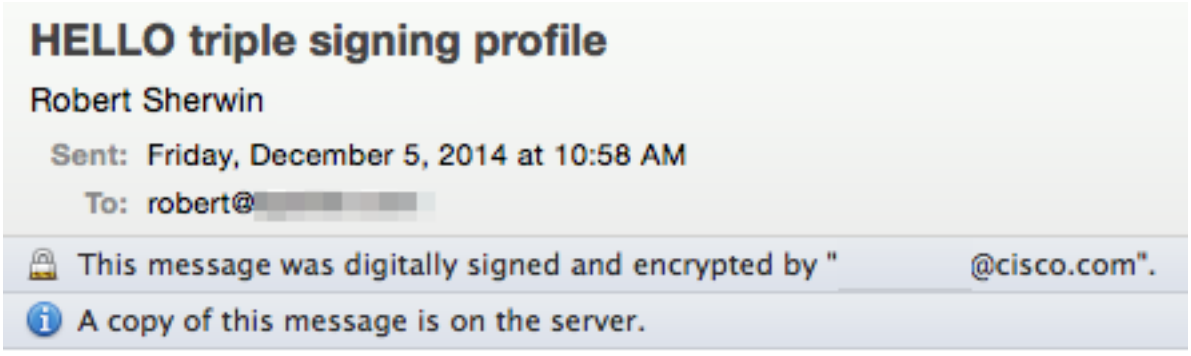
A probabilidade 2013 do exemplo como mostrado (Windows), observa o símbolo do crachá ou do certificado indicado:



O correio do exemplo como mostrado (OSX), observa que o crachá para assinado está apresentado e o cadeado para a criptografia está indicado:



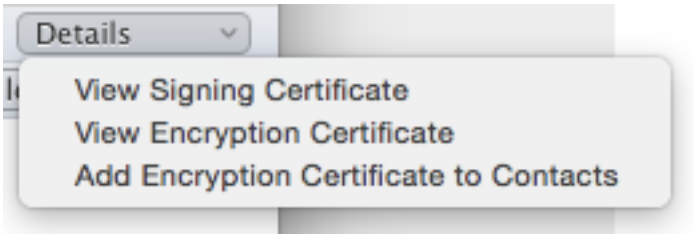
O escritório 2011 do exemplo como mostrado (OSX), observa o cadeado indicado e a mensagem, “esta mensagem digitalmente foi assinada e cifrou” incluído:



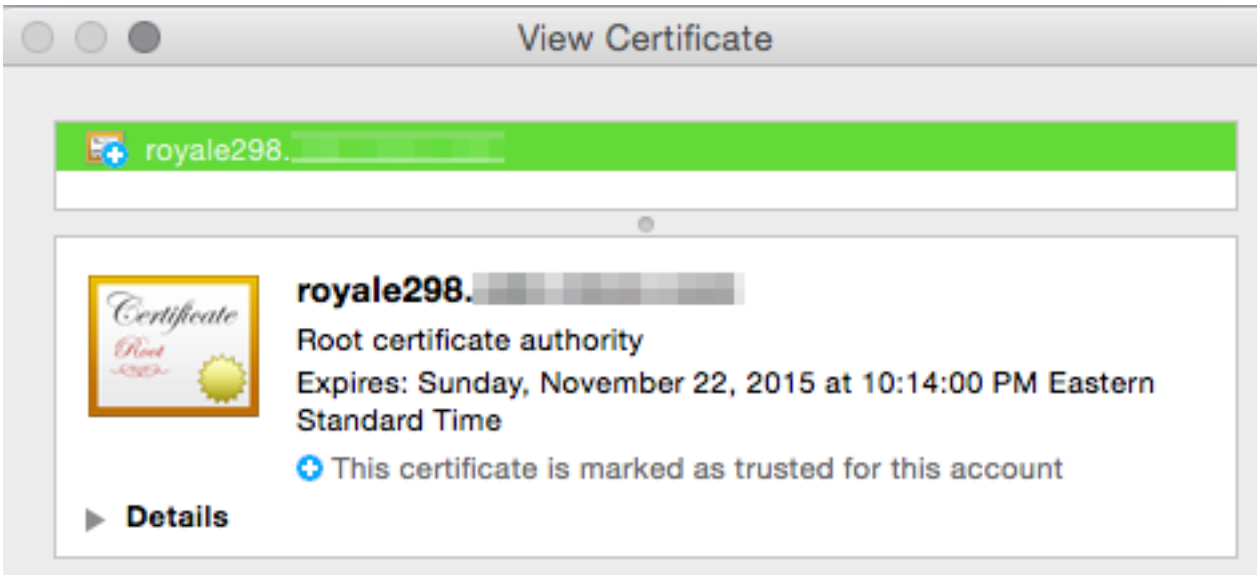
Verificação de certificado

Baseado no aplicativo de e-mail no uso, e a preferência do receptor, ou políticas de segurança da empresa, ver e aceitar o certificado variarão.

Para o exemplo acima triplo, com escritório 2011 (OSX), na linha assinada e de mensagem codificada há uma opção dropdown dos detalhes:



Selecionar o **certificado de assinatura da vista** apresenta a informação de assinatura real do certificado do ESA que esta foi enviada originalmente de:



Informações Relacionadas

- Como verificar as mensagens enviadas com o S/MIME que envia o perfil no ESA
- Suporte Técnico e Documentação - Cisco Systems
- Cisco envia por correio eletrónico a ferramenta de segurança - Guias do Usuário