DEPARTAMENTO
DE
ENGENHARIA
INFORMÁTICA

escola superior de tecnologia e gestão
instituto politécnico de leiria

www.dei.estg.iplei.pt

Sistemas de Segurança

Ficha 5 – Certificados Digitais

Nota: as imagens do Thunderbird encontram-se desactualizadas

1 Introdução

Na ficha anterior usámos o GnuPG com comandos, nesta aula vamos abordar o uso do GnuPG e o uso de certificados no cliente de e-mail Thunderbird. Embora nestes dois métodos estejam a ser usados protocolos diferentes (o OpenPGP e o S/MIME), o objectivo final é o mesmo, dar garantias de confidencialidade, integridade e autenticação aos seus utilizadores. Em ambos os protocolos são usados algoritmos de cifragem assimétrica.

A razão da escolha do Thunderbird como o cliente de e-mail para esta ficha deve-se ao facto da simplicidade de integração que este oferece com o GnuPG. No entanto existem ferramentas que permitem a integração do GnuPG (ou outra aplicação compatível com o OpenPGP) com outros clientes de e-mail. Já o S/MIME é suportado de raíz quer pelo Thunderbird, quer pela maioria dos clientes de e-mail.

2 Thunderbird

O primeiro passo será verificar se o Thunderbird está instalado. Caso não esteja deve abrir o "Adept" e pesquisar pela package "Thunderbird". A seguir deve ser configurado para a vossa conta de e-mail da ESTG. **Nota: configurar o Thunderbird para deixar uma cópia do email no servidor.**

3 Thunderbird + GnuPG

O Thunderbird não trás suporte para o GnuPG de raíz, no entanto através da instalação de uma extensão a sua integração é imediata. Para isso deve procurar no Adept a package "**mozilla-thunderbird-enigmail**" e instalá-la. Após reiniciar o Thunderbird, deverá aparecer mais um menu designado "Enigmail", esse menu e um botão designado "OpenPGP" deverão aparecer na janela de escrita de um e-mail (ver Figura 1). Depois de configurar a chave a usar podemos proceder ao envio e recepção de mensagens assinadas

e/ou cifradas. Se estivermos a compor mensagens em HTML irá surgir o aviso que está na Figura 2.

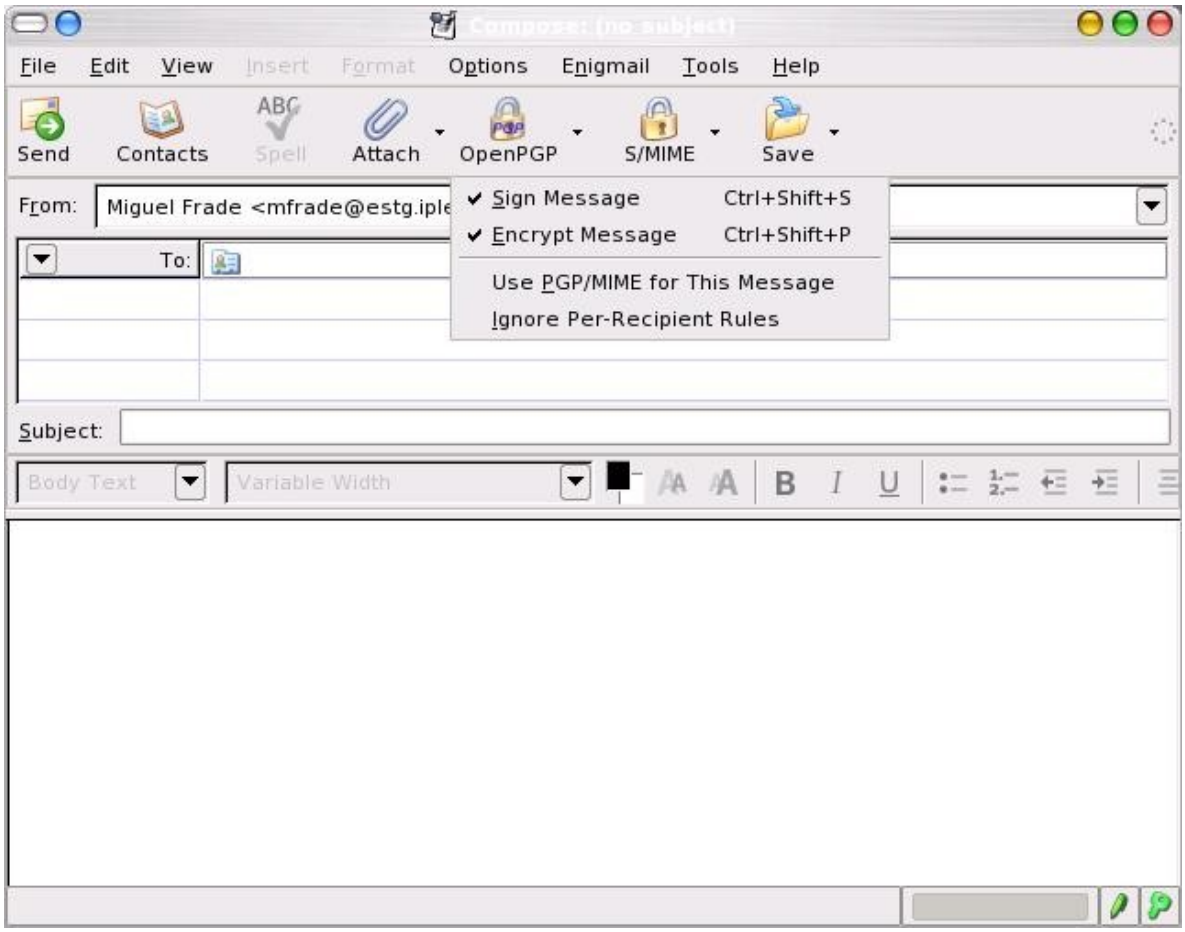

Figura 1 – Menu "Enigmail"

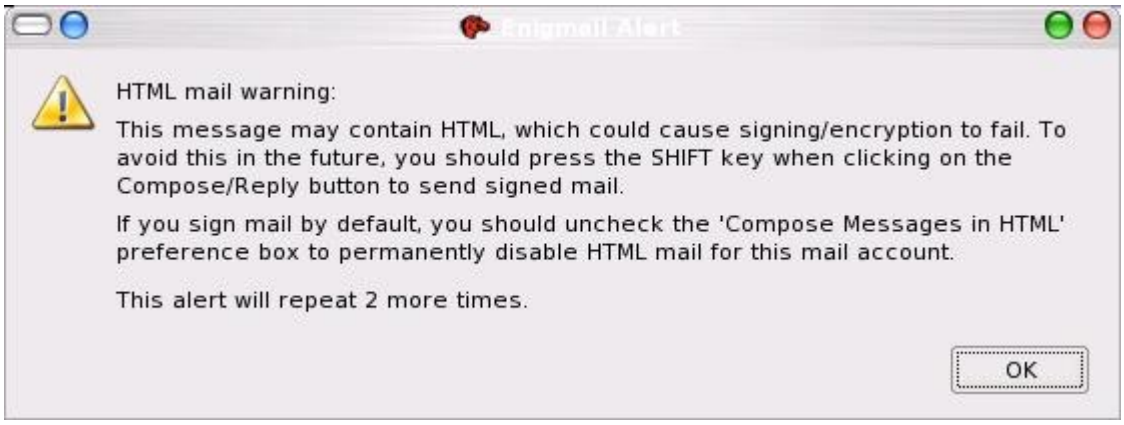

Figura 2 – Aviso sobre e-mails com HTML

O “Enigmail” tem também uma interface gráfica para a gestão de chaves (Figura 3). Para aceder a ela fazer: “Enigmail” → “OpenPGP Key Management”.

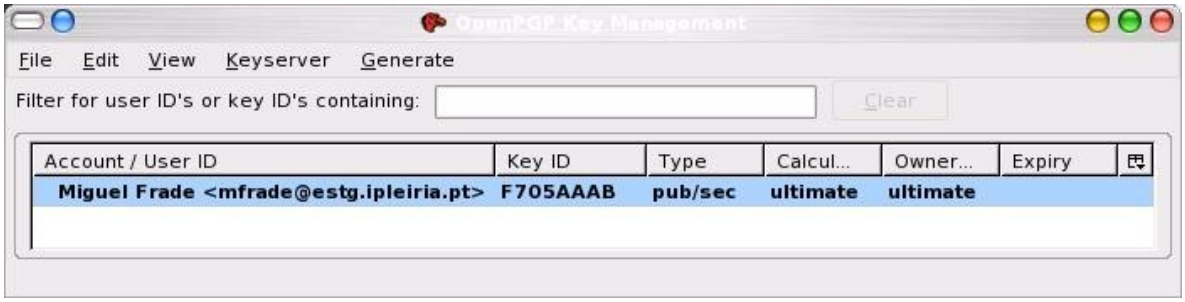

Figura 3 – Gestão de chaves a partir do “Enigmail”

3.1 Exercício

- Faça a troca de e-mails assinados e/ou cifrados entre os colegas.
- Teste a importação de chaves públicas dos colegas
- Aceda a “Enigmail” → “Preferences” → “Sending” e faça o envio de mensagens cifradas com a opção “Encrypt to self” activa e desactiva. Aceda à pasta do Thunderbird onde são guardadas as mensagens enviadas e compare as mensagens guardadas nessa directoria com a opção activa e desactiva.

4 Thunderbird + S/MIME

Como já foi referido anteriormente, o Thunderbird já trás suporte ao protocolo S/MIME. Este protocolo, não é mais do que uma extensão ao MIME para suporte de certificados digitais X.509. Estes protocolos serão abordados de forma mais aprofundada nas aulas teóricas.

O primeiro passo será a obtenção de um certificado digital, para isso os alunos devem aceder ao site http://www.cacert.org e fazer o “Join”. Aí serão pedidos vários elementos identificativos e depois será enviado um e-mail sonda. Só após a recepção do e-mail de sonda ter sido recebido e o aluno ter seguido o link dentro desse e-mail é que o processo de adesão fica concluído. Este certificado não contém o nome do aluno e certifica apenas a existência do endereço de e-mail especificado e são válidos por um ano.

Enquanto se aguarda a chegada do e-mail sonda, devemos efectuar a instalação do certificado digital da CA. Este passo é necessário devido ao facto deste certificado não vir pré-instalado nem nos browsers, nem no Thunderbird (ao contrário do que acontece com outras CA’s, como por exemplo a VeriSign). Os passos a seguir são:

- Aceder à página http://www.cacert.org e clicar sobre o link “Root Certificate” (que se encontra do lado direito da página)

- Guardar o ficheiro que se obtém ao clicar sobre “Root Certificate (PEM Format)”

- No Thunderbird ir ao menu “Edit” → “Preferences” → “Advanced” (Figura 4), clicar sobre o botão “Manage Certificates ...”

- Seleccionar o separador “Authorities” (Figura 5) e clicar sobre “Import” e seleccionar o ficheiro com o certificado da CA.

- A seguir deverá aparecer uma janela onde indicamos para que situações é que confiamos na CA em causa (Figura 6). No entanto antes de escolhermos qualquer opção devemos clicar sobre o botão “View”

- Na nova janela (Figura 7) estão listados vários dados sobre o certificado da CA onde se destaca os fingerprints MD5 e SHA-1. Antes de aceitar este certificado deve verificar se o fingerprint coincide com o apresentado na página da CAcert.org.

- O passo seguinte é verificar se a instalação foi bem sucedida, para isso procurar por “Root CA”, como está na Figura 8.

- Depois destes passos já deverá ter recebido o e-mail sonda derivado do seu processo de adesão à CAcert.org. Deverá concluir a adesão seguindo o link indicado nesse e-mail.

- Após a conclusão da sua adesão deve fazer a instalação do seu certificado. Este passo pode ser feito de duas formas: uma delas é esperar por um e-mail da CAcert com um link directo, a outra é aceder à página da CAcert.org → “Normal Login” → “Client Certificates” → “View”. Depois clique sobre o seu endereço de e-mail.

- Qualquer que seja o passo escolhido deverá estar numa página com o título “Installing your certificate”. Aqui deve clicar sobre o link “Click here” e provávelmente não obterá nehuma resposta do browser. Deverá manualmente verificar se o seu certificado ficou instalado ou não. Se por acaso não ficou a melhor maneira é repetir este passo com outro browser, por exemplo o Firefox (cuja interface de gestão de certificados é igual ao Thunderbird).

- No browser onde conseguiu fazer a instalação do seu certificado deverá exportá-lo para um ficheiro com a extensão “p12”. Se o browser for o Firefox a janela com o certificado tem o aspecto da Figura 9. Aí deve escolher o certificado e depois a opção “backup”.

- O último passo será importar o certificado do utilizador para o Thunderbird. Este passo é semelhante à importação do certificado da CA (Figura 5), mas desta vez no separador "Your Certificates"

Figura 4 – Gestão de certificados

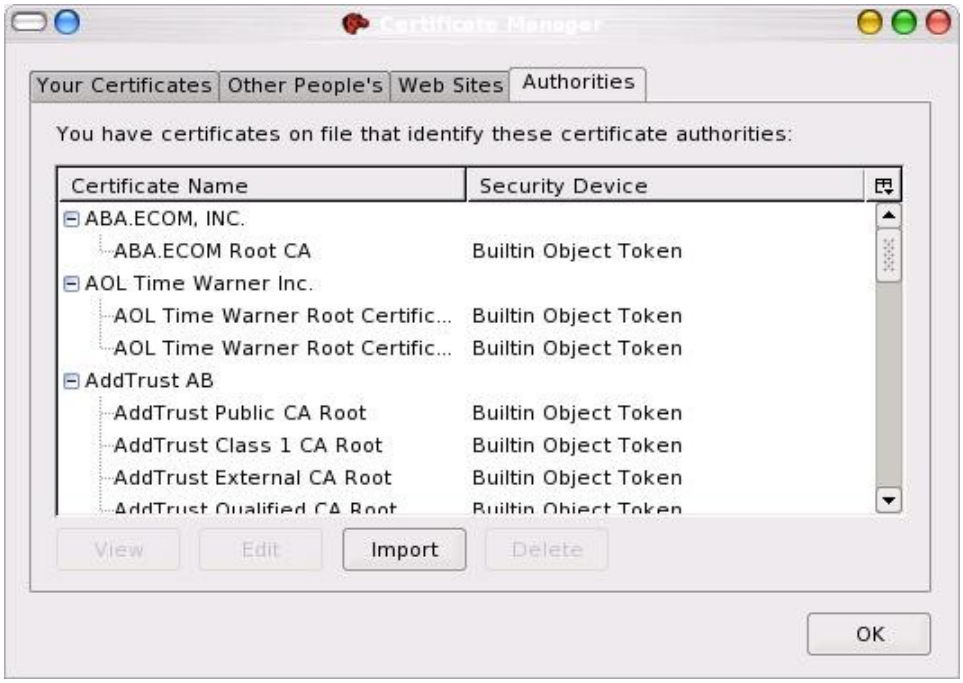

Figura 5 – Importar certificado da CA

Figura 6 – Confiança na CA

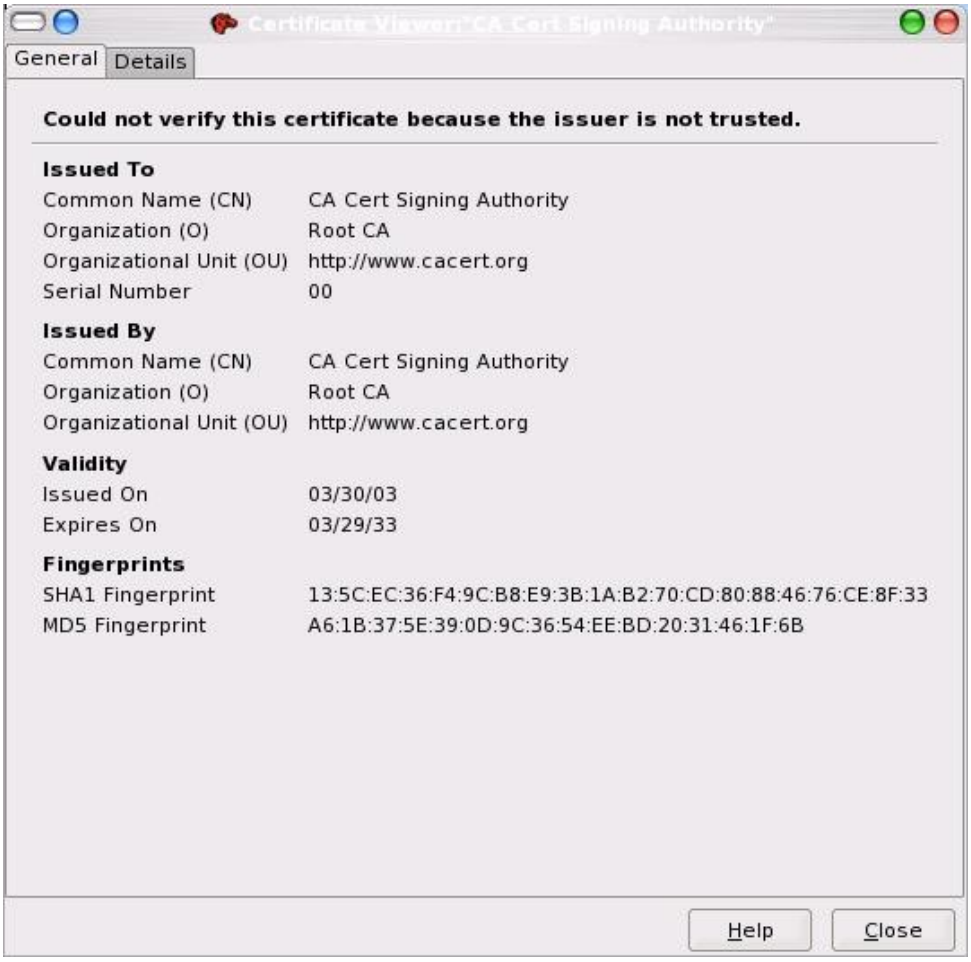

Figura 7 – "Fingerprints" do certificado da CA

Figura 8 – Verificação da instalação do certificado da CA

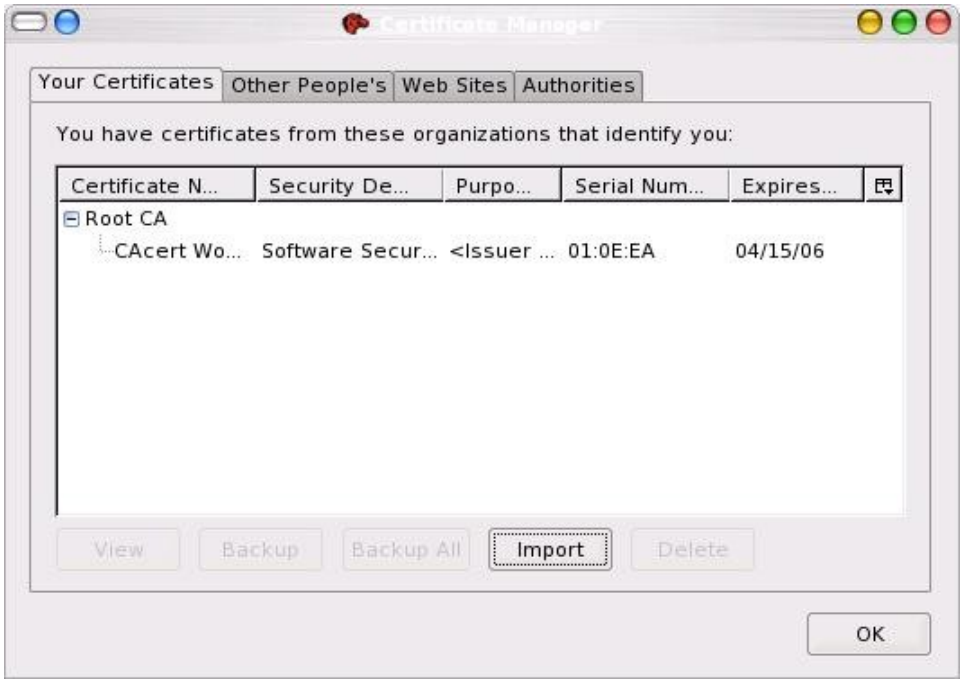

Figura 9 – Verificação da instalação do certificado do utilizador

4.1 Exercício

Após ter completado todos os passos poderá começar a enviar e-mails usando o seu certificado. Para isso deverá usar as opções do menu "Security" (ou "S/MIME" após a instalação do Enigmail), como na Figura 10. Na primeira tentativa de envio de e-mail com certificados é natural que surja uma mensagem de aviso para configurar o certificado a usar.

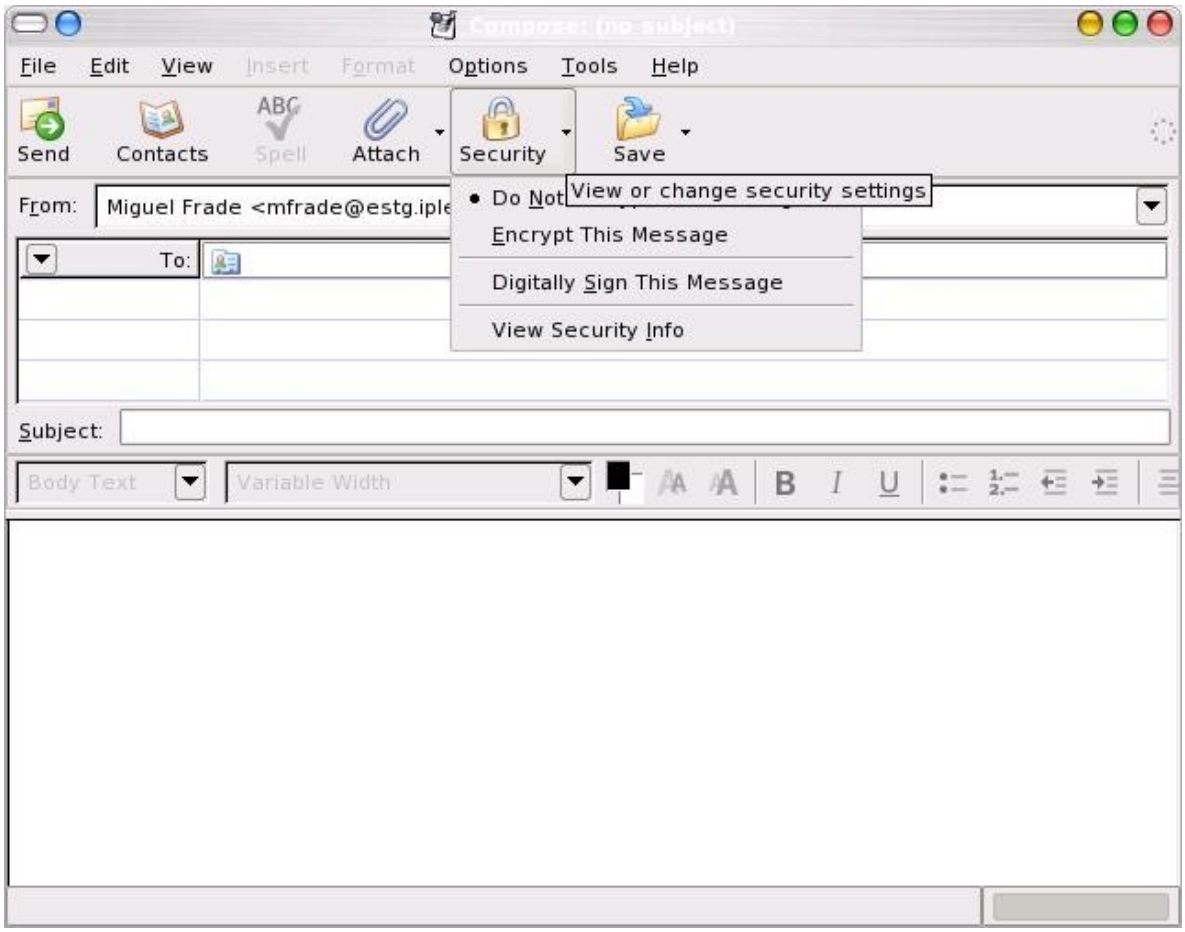

Figura 10 – Opções de segurança relativas aos certificados (o nome do botão muda para S/MIME após a instalação do Enigmail)

- Faça a troca de e-mails assinados e/ou cifrados entre os colegas.
- Teste a importação de certificados dos colegas