


TP2: Cifra, assinaturas, certificados e o ADSS

Notas:

1. Os conceitos apresentados nesta ficha de trabalho, assim como os exercícios propostos, complementam o material facultado na componente teórica e não deve ser utilizado sem um claro entendimento dos conteúdos aí apresentados. **Para efeito da apresentação de resultados, deverá registar as suas observações num *logbook*, no mínimo referentes às tarefas assinalados a vermelho.** A avaliação será feita com base no *logbook* e por isso o mesmo deve ser claro e objetivo.
2. Na realização deste trabalho necessita apenas de um computador pessoal com ligação à Internet e acesso a algumas aplicações, entre elas um cliente de email que permita cifrar e assinar emails recorrendo a certificados X.509 (e, desejavelmente, também certificados PGP), um servidor de PKI (no nosso caso o ADSS CA Server / PKI Server, da Ascertia) e um programa que permita gerar um par de chaves (recomenda-se o OpenSSL). O PGP (ou o GnuPG, ou ainda o GPG4Win) permite fazer as mesmas tarefas mas sem recorrer a uma PKI, conforme detalhado durante as aulas¹. A instalação do software não é contemplada nas tarefas propostas nesta ficha. No contexto das definições e trabalhos seguintes, o conceito de “chave” e de “certificado” associado não estão claramente diferenciados, por ser esse o entendimento que muita da documentação disponível assume.
3. O servidor ADSS (Advanced Digital Signature Service) é um produto da Ascertia que fornece serviços de geração e verificação de assinaturas digitais, validação de certificados e outros serviços relacionados com a gestão de uma PKI. Existe uma instalação disponível na UM (para fins pedagógicos e de investigação) disponível a partir de <https://e-tslab.dsi.uminho.pt:8774/adss/console>
Para aceder ao servidor deverá estar a usar a rede da UM (diretamente ou por VPN) e instalar no seu browser um certificado de autenticação do grupo, que lhe será entregue no início do exercício – **este é o único processo para fazer login no servidor e utilizar a consola de administração.** A documentação do servidor está acessível a partir de https://e-tslab.dsi.uminho.pt:8774/adss/console/docs/help/getting_started.htm
4. A utilização do símbolo  denota afirmações que podem fazer parte de uma política de segurança.

¹ NOTA: Existe uma grande semelhança ao **nível funcional** entre a versão pública do PGP (versão 8.0.2), a versão *trial* do PGP (agora fornecida pela Symantec ☺) e o GnuPG, apesar de os respectivos interfaces serem diferentes; este trabalho pode ser realizado utilizando o ambiente gráfico, mas é igualmente possível (e até mesmo aconselhável) utilizar o GnuPG. Neste caso será necessário ter o cuidado de adaptar as instruções ao interface do GnuPG.

As versões *freeware* do PGP estão disponíveis em <http://www.pgpi.org/products/pgp/versions/freeware/>
A versão *trial* está disponível no site da Symantec - estamos interessados no “PGP Desktop Email”, sendo necessário criar uma conta e licenciar (gratuitamente, por 30 dias) o produto, que estará então disponível com algumas limitações mas que não comprometem a realização deste trabalho.


O GnuPG está disponível em <http://www.gnupg.org/>

O GPG4Win está disponível em <http://www.gpg4win.org/>


Antes de começar

1. Verifique se tem acesso ao servidor ADSS (deve ter um certificado de autenticação que lhe foi entregue pelo administrador do servidor; deverá ainda estar a utilizar o servidor a partir da rede da UM, ou de um acesso VPN).
2. Cada membro do grupo deve começar por gerar um “**par de chaves**”. Este par de chaves é composto por uma **chave pública** (a disponibilizar publicamente, através de um certificado) e uma **chave privada** (a guardar cuidadosamente). Localmente existirá sempre um local no disco onde todas as chaves públicas (certificados) são armazenadas e um local separado onde as chaves privadas são armazenadas – naturalmente, este último local e a forma como as chaves são armazenadas, constitui um aspeto crítico do funcionamento do sistema.

No caso do PGP e no Windows, esses ficheiros são designados por **kryrings**; um deles – `pubring.pkr` – armazena todas as chaves públicas de utilizadores para quem pretende enviar mensagens de forma segura, o outro – `secring.skr` – armazena a(s) chave(s) privada(s). Estes ficheiros estão armazenados de uma forma cifrada, no espaço de trabalho do utilizador, (...\\My Documents\\PGP, no Windows); simples... talvez demasiado!

 A utilização de mais do que um par de chaves justifica-se quando se pretende utilizar mais do que uma assinatura - podemos querer utilizar uma assinatura pessoal e uma outra assinatura institucional, apenas com alguns elementos de identificação comuns – ou quando queremos estabelecer canais de comunicação seguros e exclusivos, com várias entidades.

3. O **OpenSSL**² é um conjunto de ferramentas extremamente poderoso para explorar diversas aplicações de chaves de cifra. Recomenda-se a sua utilização ao longo deste trabalho e, bem assim, a consulta da documentação associada que ajuda a compreender vários aspetos mais complexos – em particular a secção de HOWTOs pode ser muito útil.
4. Em diversas aplicações, ao gerar um par de chaves na realidade poderá estar a associar várias chaves: uma chave privada ("Mestra") para assinaturas - habitualmente com o algoritmo DSS e destinada apenas a assinar chaves públicas; uma segunda chave, ou melhor uma **subchave**, para cifrar; e uma ou mais subchaves adicionais, para a assinar, cifrar ou assinar/cifrar (se tentar usar o PGP irá poder verificar isso mesmo).

 Este procedimento permite, por exemplo, manter as assinaturas de chaves públicas válidas durante um largo período de tempo e modificar a subchave de cifra e/ou de assinatura de documentos regularmente (talvez períodos de um ano). Este pode ser um procedimento de segurança muito útil.

Additional Decryption Keys (ADKs) são chaves de decifra adicionais, que permitirão aos responsáveis da segurança de uma organização, decifrar mensagens cifradas para a chave pública associada à ADK. Na prática, é uma segunda chave que pode decifrar.

Em princípio, estas chaves só serão utilizadas em caso de extrema necessidade!

Corporate Signing Key é uma chave pública atribuída a uma organização e na qual todos os utilizadores, relacionados de alguma forma com essa organização, podem confiar.

² <https://www.openssl.org/docs/>

Todas as chaves assinadas pela correspondente **Corporate Key** (chave privada) podem ser assumidas como válidas – enquanto as não assinadas devem ser assumidas com bastante precaução.

5. Validação de uma chave: quando importamos uma cópia de uma chave pública de “alguém”, ou melhor, o seu certificado, podemos adicioná-la ao nosso *keyring*. Mas antes de a usar para cifrar alguma mensagem temos que proceder à respetiva **validação** (determinar se a identificação existente na chave pública corresponde à pessoa física com quem nos queremos relacionar):
- a) Se a chave foi entregue pessoalmente, é válida;
 - b) Se foi entregue por e-mail ou obtida a partir de um servidor:
 - i) Se vem assinada por alguém em quem confiamos, será válida (é o caso de uma chave assinada por uma CA);
 - ii) Em caso de dúvida devemos contactar a pessoa em questão e pedir-lhe que nos indique a “impressão digital” do seu certificado, comparando-a com a que consta na chave que temos em nosso poder (a Figura 1 ilustra o *fingerprint* de um certificado PGP, como exemplo). Se a verificação tiver sucesso a chave é válida;
 - c) No caso de não se usar uma CA, o resultado do processo de validação deve ser registado no certificado, o qual deve ainda ser assinado por si (caso seja válido) e reenviado para a base de dados, por forma a dar conhecimento do nosso “parecer” – esta é a essência do **web of trust**;
 - d) Em caso de dúvidas sobre a validação deve ser registada a indicação “Inválido” no certificado, o que impedirá o seu uso.

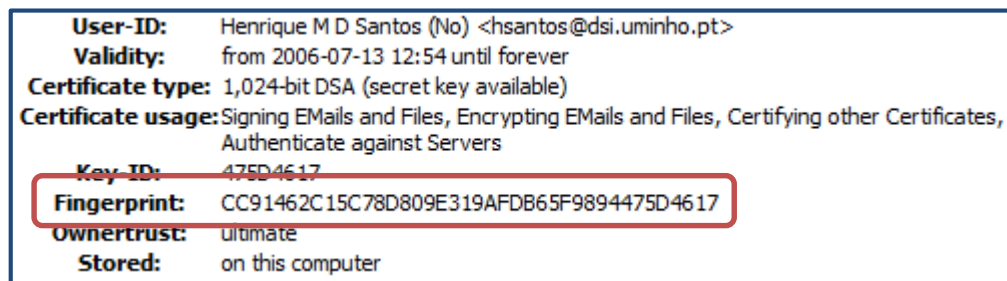


Figura 1- Verificação da fingerprint nas propriedades de uma chave

Objectivos

1. Descrever a forma como o conceito de chave pública é tipicamente implementado.
2. Reconhecer as operações associadas à gestão das chaves públicas e privadas.
3. Desenvolver competências na utilização do ADSS CA Server (e, eventualmente, do PGP).
4. Utilizar certificados para enviar e receber mensagens de email, com segurança.

Exercícios

Gestão de chaves:

1. Prepare e inicie a sua ligação ao servidor ADSS. A ligação à consola deste servidor é autenticada (SSL com autenticação do cliente) através de um certificado pessoal, com chave privada, que lhe será disponibilizado (ficheiro PKCS#12, que contém chave pública e privada, **<curso-grupo.pfx>**, onde **<curso-grupo>** identificará o seu grupo de trabalho). O perfil com que se ligará dá-lhe acesso limitado às funções relevantes para este trabalho (gestão de chaves, gestão de CAs locais e verificação de *logs*). Assim, antes de tentar ligar ao servidor deve instalar no *browser* o certificado – consulte as instruções de instalação para o *browser* que está a utilizar. Pode agora ligar-se ao servidor (desde que esteja na rede interna da UM) através do URL: <https://e-tslab.dsi.uminho.pt:8774/adss/console>

Nota: Depois de testar faça *logout* do servidor para permitir que o mesmo possa ser usado pelos colegas, uma vez que apenas 1 grupo o pode usar em cada instante – todos partilharão o certificado atrás referido (se esta limitação for entretanto ultrapassada, tal será devidamente comunicado).

2. Instale o OpenSSL (por defeito, a maioria das imagens do bem conhecido Ubuntu, ou relacionadas, já trazem este pacote de software instalado). Poderá utilizar qualquer outro *software* alternativo que tenha a capacidade de gerar um par de chaves, pública e privada, mas no resto deste exercício assume-se que está a utilizar o OpenSSL. Caso use uma alternativa, deverá adaptar os comandos/ações para o seu ambiente.
3. Crie um novo par de chaves. Se usar o OpenSSL e quiser obter um par de chaves RSA, deverá executar o comando (ou alguma variante) `openssl genrsa -out privkey.pem 2048`, o qual irá criar uma chave privada e a associada chave pública, de 2048 bits, ambas guardadas no mesmo ficheiro, do tipo PEM³. A chave assim obtida é adequada para poder cifrar e assinar e não necessita de palavra-passe para ser utilizada, o que no contexto da geração de certificados, que podem ser manuseados por servidores, é uma boa opção – mais sobre este assunto pode ser consultado na documentação do OpenSSL⁴.

Verifique o bom estado da sua chave privada com o comando

`openssl rsa -in privkey.pem -check`

e registe a resposta do comando, que inclui o “texto” com a sua nova chave privada.

4. Com vista à integração numa PKI, de seguida deverá preparar um ficheiro com um pedido de certificado. Este pedido incluirá a sua chave pública, associada à chave privada anteriormente gerada, alguma informação pessoal e organizacional (a maior parte com carácter opcional) e alguns atributos, entre eles o *Common Name* (CN) e o endereço de email (aspetos de identificação particularmente importantes, como é óbvio), que serão também incluídos no seu certificado. Será este ficheiro que irá enviar para a Autoridade Certificadora (CA), a qual, depois de validar a sua identidade, devolverá o certificado assinado por ela.

³ De uma forma resumida, os ficheiros PEM contém informação binária codificada em ASCII, o que facilita o seu manuseamento (copy/paste) com ferramentas simples de processamento de texto.

⁴ <https://www.openssl.org/docs/HOWTO/keys.txt>

No OpenSSL pode gerar o pedido de certificado usando o comando:

`openssl req -new -key privkey.pem -out cert.csr` (ajustando devidamente os nomes dos ficheiros, conforme a sua escolha), que lhe irá gerar um pedido com o formato PKCS#10, um *standard* que a grande maioria das CA aceita.

Verifique o estado do seu ficheiro de pedido de certificado com o comando

`openssl req -text -noout -verify -in cert.csr`

e registe a resposta do comando, que inclui os atributos do seu pedido e do futuro certificado.

5. O OpenSSL permite-lhe ainda gerar uma chave privada e um certificado auto assinado (X.509) por essa chave privada, para utilização privada ou no contexto de um conjunto de relações locais, para o qual não é necessário (nem desejável) ter uma entidade de topo a assinar o seu certificado – este é o princípio de funcionamento subjacente à alternativa de certificação gerada pelo PGP (*web of trust*), mas é também a alternativa para o certificado de topo de uma CA! Por outro lado, o formato assim obtido é frequentemente necessário para importar a sua chave privada para qualquer ambiente. Para gerar o certificado pode então usar o comando:

```
openssl x509 -req -in cert.csr -signkey privkey.pem -out
privcert.crt
```

O certificado assim obtido é válido por um ano (a opção `days` pode ser usada para criar certificados com durabilidade diferente).

6. Os passos 3 a 5 devem ser executados por cada um dos elementos do grupo, para que cada um fique com um par de chaves e um pedido de certificado, em seu poder. O passo seguinte consiste em pedir o certificado público, devidamente assinado por uma CA. Mas neste exercício a CA vai ser criada e gerida pelo próprio grupo ☺. Para tal devem aceder novamente à consola do servidor ADSS, conforme já descrito. O primeiro passo agora é gerar um certificado da CA. Para isso aceda à função **Key Manger** e selecione a opção **Service Keys**. Vai então criar um novo par de chaves, selecionando o botão **New**, o qual fará aparecer uma janela onde deve preencher duas importantes descrições: **Key Alias**, onde deve dar um nome ao novo par de chaves – xxxGrupoN, onde xxx deve ser substituído pelas siglas da UC e N pelo número do grupo; e **Purpose**, onde, através da lista de alternativas, deve escolher **Certificate/CRL Signing**, já que este certificado servirá exclusivamente para assinar certificados públicos. Por questões de segurança NÃO deve ativar a possibilidade de exportar a chave privada deste certificado, que será exclusivamente usada pelo servidor – outra coisa não faria sentido, certo?
7. De regresso ao ecrã do **Service Keys**, já deverá ver, entre outros, o par de chaves que acabou de criar. Selecione agora (*radio button*, à esquerda) o par de chaves da sua futura CA e selecione desta feita o botão **Certificates** (ou selecione diretamente o par de chaves através do **Key Alias**). Como não tem qualquer certificado associado a este par de chaves, a lista aparece vazia. Escolha então a opção **Create CSR/Certificate**, o que o levará a uma janela onde deve preencher a informação do certificado, à semelhança do que fez anteriormente com o OpenSSL. No campo **Certificate Alias** deve dar um nome significativo ao certificado – sugere-se o mesmo nome do par de chaves, seguido de “-CA”, o que facilitará a sua identificação; ao fundo deve ainda selecionar a opção **Create Self-Signed Certificate**; no campo **Email** deverá colocar o endereço de correio eletrónico de um dos elementos do grupo; tudo o resto é opcional, mas aconselha-se a incluir o nome da organização (“UMinho”), da unidade (“DSI”) e o país; finalmente, repare que o *template* está previamente selecionado e que não o pode alterar. Para efeitos de registo:

Faça um *print screen* parcial do ecrã, com toda a informação inserida, antes de terminar com **OK**.

8. Após criar o certificado e voltando ao ecrã **Key Manager > Service Keys**, selecionando novamente o par de chaves da sua CA já verá o certificado que acabou de criar. Através do **Certificate Alias** selecione o certificado e **registre no seu logbook as propriedades do certificado, bem como a chave pública**. Pode ainda transferir (**Save**) o certificado para um ficheiro, o que pode igualmente fazer através da função **Export**, na janela anterior. Poderá ser boa ideia caso tenha algum *software* que precise de verificar a assinatura da CA, num certificado público de outro elemento.
9. Selecione agora a função **Manage CAs** e, de seguida, a opção **Configure Local CAs**. Na coluna **CA Friendly Name** poderá ver já várias CAs, mas nenhuma (esperemos) com o nome da “sua” CA. No entanto, pode selecionar algumas das já existentes e ver os certificados associados. Para criar uma nova CA selecione o botão **New**. Atribua um nome à nova CA (este campo é obrigatório e sugere-se que use o mesmo nome que usou no certificado), e escreva uma breve descrição, se entender apropriado ☺. Selecione o certificado da CA da lista e **TENHA CUIDADO PARA SLECIONAR O CERTIFICADO QUE CRIOU ANTERIORMENTE** (caso contrário poderá ter dificuldades posteriormente, como é natural). Aproveite para ver as restantes propriedades, em particular o que diz respeito à CRL (*Certificate Revocation List*), essencial para o funcionamento de uma CA “a sério” – pode ativar a geração automática e publicação da CRL (use como **CRL Publishing File Path** `/var/www/html/certificados/file.crl`, mas usando um nome de ficheiro apropriado ao seu caso) e diminuir o tempo de renovação (mas tenha cuidado porque está em minutos!). Finalmente e para efeitos de verificação dos certificados, preencha o campo **CDP Address (http)** com “`http://e-tslab.dsi.uminho.pt/certificados`”, o que ficará como uma extensão aos certificados assinados pela sua “CA”, permitindo aos diferentes clientes automaticamente solicitar a verificação do estado de um certificado (caso o cliente o suporte, naturalmente). **Antes de selecionar o botão Ok, tire um print screen com a informação que inseriu e copie para o seu logbook.**
10. De regresso ao ecrã **Manage CAs**, resta agora assinar as chaves públicas individuais anteriormente geradas (passos 2 a 5), para obter os respetivos certificados, de todos os elementos do grupo. Selecione a opção **Manual Certification**. Todos os campos são obrigatórios e relevantes:
 - I. **Certificate Alias**: o nome (curto) do utilizador que requer o certificado;
 - II. **Certificate Template**: o fim a que se destina o certificado; sugere-se o Default SMIME Template, que se adequa bem à função desejada (verifique o *template* e aproveite para ver outros *templates*, comparando-os);
 - III. **CA Certificate**: deverá selecionar o certificado da sua CA
 - IV. **Import PKCS#10**: escolha o ficheiro com o pedido de certificado, gerado para um dos elementos do grupo.

Imediatamente após a criação do certificado recebe a mensagem de sucesso (se tudo correu bem), tendo então a possibilidade de ver o certificado, descarregar o certificado para um ficheiro – afinal é um certificado público, que pode instalar em qualquer SO ou cliente de Email, ou distribuir manualmente – ou ainda descarregar para um ficheiro especial a cadeia de certificação usada. Como é óbvio, a operação acima descrita deve ser repetida para cada um dos elementos do grupo.

11. Uma vez concluída a tarefa anterior, regresse ao ecrã **Manage CAs** e selecione a opção **Configure Local CAs**. Selecione a sua CA da lista e selecione o botão **Issued Certificates**. Copie para o logbook o resultado obtido. Está de acordo com o que esperava? Caso identifique discrepâncias, procure justificá-las.

Selecione ainda cada um dos certificados gerados pela sua CA (também aqui tem a possibilidade de visualizar o mesmo, assim como guardar uma cópia em ficheiro). Copie para o logbook os certificados públicos assinados.

12. De regresso ao OpenSSL e porque para importar a sua chave privada em diferentes aplicações irá muito provavelmente precisar de um ficheiro no formato PKCS#12, deverá ainda usar o comando: `openssl pkcs12 -export -in pubcert.pem -inkey privkey.pem -certfile CAcert.pem -name "my-name" -out priv-pkcs12.p12` onde:

- `pubcert.pem` é o seu certificado público, assinado pela CA, no formato PEM – muito provavelmente terá este certificado no formato X.509 e, para o converter, pode usar o comando `openssl x509 -inform der -in cert.cer -out cert.pem`
- `privkey.pem` é a sua chave privada
- `CAcert.pem` é o certificado da CA, no formato PEM (também pode precisar de o converter)

Ao executar o comando será-lhe pedida uma palavra-chave, a qual servirá para o autenticar quando importar a chave privada e, por opção sua, sempre que for necessário usar a sua chave privada (não é necessário realçar a importância desta palavra-chave!). Como é lógico, cada aluno tem que repetir este processo para poder importar a sua chave privada.

Os passos seguintes dependem grandemente do ambiente que estiver a usar. As sugestões apresentadas confinam-se a um único ambiente e terá que ajustar/pesquisar as soluções que se ajustem ao seu ambiente.

13. Neste momento cada grupo tem uma CA, o respetivo certificado público, os certificados públicos de cada aluno, assinados pela sua CA e as respetivas chaves privadas armazenadas em ficheiros PKCS#12 (que ainda contém um certificado público assinado pela CA ☺). Em ambiente Windows qualquer um dos certificados gerados pode ser importado, bastando para tal executar um duplo *click* sobre o respetivo ficheiro e seguir as indicações que aparecem no ecrã. Se percebeu cabalmente o que fez, sabe que no ficheiro PKCS#12 que gerou tem todos os elementos que precisa para instalar a sua chave privada e o seu certificado público, assim como o da sua CA. Posteriormente pode fazer a gestão dos certificados usando uma MMC (*Microsoft Management Console*), chamada **certmgr.msc** (que pode executar diretamente da opção **Run** do botão **Start** do Windows, ou de qualquer forma equivalente – a Figura 1 mostra um exemplo da janela dessa consola), ou a partir do **Control Panel**, opção **Internet Options**, e *tab* **Content**. Instale todos os certificados públicos no seu Sistema Operativo e o seu certificado privado. Localize a informação relevante no gestor de certificados e registe a localização no seu logbook.

Quando abre um dos certificados que importou (exceto o pessoal), o Windows poderá reportar que não é válido, uma vez que não reconhece a CA de topo (isso acontece se não inclui no ficheiro PKCS#12 obtido anteriormente o certificado da CA e/ou não instalou corretamente esse

certificado. Se isso acontecer deverá fazer a instalação manualmente. **Procure e documente, se for caso disso, uma forma de forçar o Sistema Operativo a considerar válidos os certificados.**

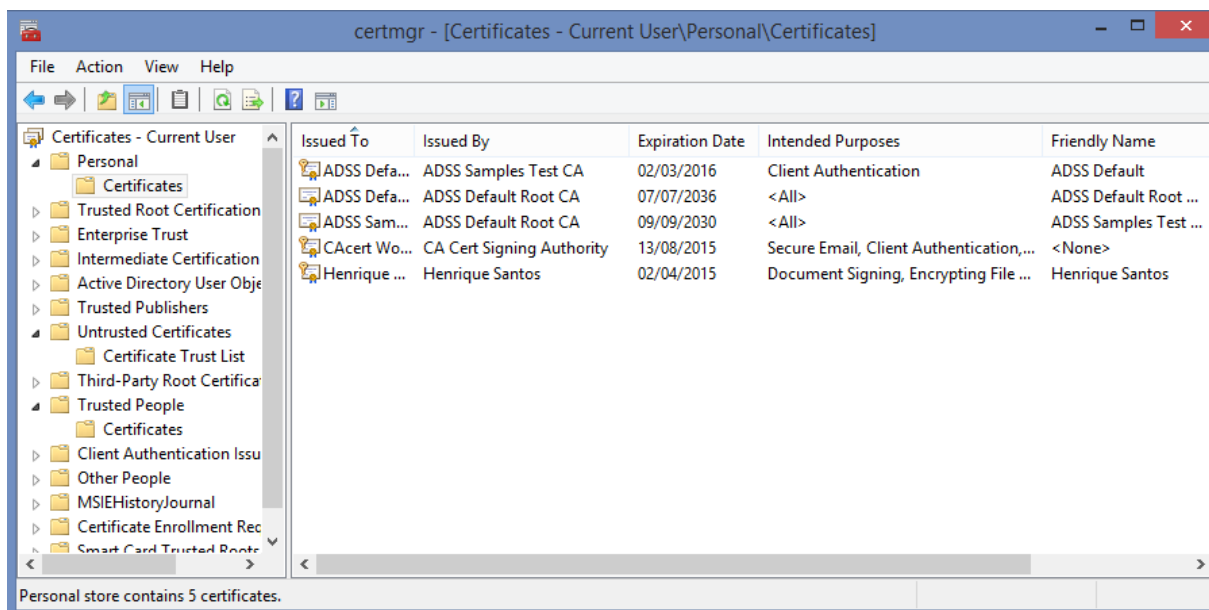


Figura 2 - Janela típica do gestor de certificados do Windows, certmgr.msc

A grande maioria das aplicações que permitem cifrar/decifrar e assinar documentos usam a infraestrutura do Sistema Operativo (e.g., Outlook e Acrobat Reader). Assim, a partir deste momento, estará em condições de executar algumas experiências práticas.

Enviar e receber mensagens seguras

Neste exercício iremos utilizar, como referência, o cliente Thunderbird. Contudo, graças à integração por *plugins*, a descrição aplica-se a vários outros clientes (obviamente a menos das figuras aqui mostradas ☺), tais como o Windows Live Mail, o Eudora, ou o eM Client – em alguns casos poderá sentir alguns problemas com a validação do certificado privado...

14. Para começar tem que indicar ao cliente de Email qual o certificado com a sua chave privada e que pretende usar (isto porque poderá ter vários). No menu **Tools** escolha a opção **Account Settings**. De entre os grupos de configurações disponíveis, escolha **Security**. Tem agora a possibilidade de:

- I. Gerir os certificados que dispõe no seu computador, através da opção **View Certificates** (ver Figura 3); pode ver os seus próprios certificados (chave pública e privada, tipicamente), os de outras pessoas, os de servidores, os de CAs reconhecidas e outros; tem ainda a possibilidade de importar certificados, para qualquer das classes anteriores – o que precisará de fazer, para poder usar a sua chave privada.
- II. Escolher o certificado que pretende usar para assinar e para decifrar (embora possam ser diferentes, na maioria dos casos é o mesmo).

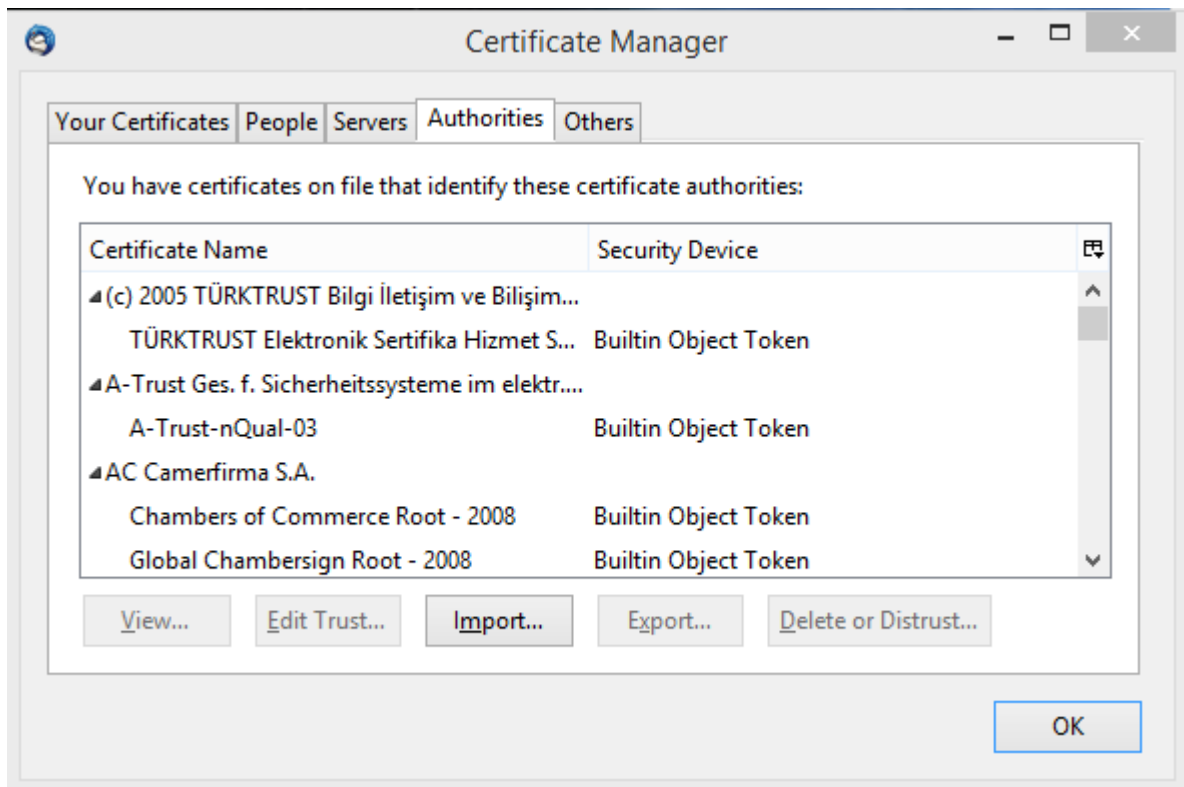


Figura 3 - Gestor de certificados do Thunderbird

Tenha em atenção que (1) o cliente de email usa habitualmente o endereço de email para escolher os certificados. Se o seu certificado de assinatura tem um endereço de email diferente do que usa para enviar email, poderá não conseguir assinar mensagens! (2) se alguém lhe enviar um certificado público por email, ele será automaticamente guardado, desde que a CA seja reconhecida – no seu caso isso não acontecerá, porque a CA que criou é fictícia e não está devidamente registada; mas pode efetivamente “forçar” o seu sistema a reconhecer e aceitar a sua CA, bastando para isso carregar o respetivo certificado público na categoria de Autoridades.

A utilização do webmail não permite, habitualmente, executar este tipo de operações, assumindo-se que tal é feito no computador pessoal, ao nível do ficheiro, usando algum software para o efeito. Como exemplos refira-se a *suite* de segurança iSafeguard™ e o GPG (já anteriormente referido, mas que está orientado à utilização de certificados PGP). Para fazer assinaturas digitais o Adobe Reader serve perfeitamente, assim como o HelloSign (uma aplicação web que integra muito bem com o ambiente Google).

Configure devidamente os diversos clientes de email dos elementos do grupo e exercitem a troca de mensagens, com a assinatura e cifra. Deverão documentar todas as experiências no logbook.

15. O exercício seguinte consiste em revogar um dos certificados e verificar o que acontece. Para isso deve regressar à consola do ADSS. Na função **Manage CAs** e na opção **Configure Local CAs** tem acesso a todas as CAs (não se esqueça que existe um único perfil de acesso, pelo que o servidor não distingue os utilizadores). Selecione a sua CA e, de seguida, aceda aos certificados emitidos, através da opção **Issued Certificates**. Agora basta selecionar o certificado que lhe interessa e executar a operação **Revoke**. Indique a data e hora de revogação (tem que ser anterior ao momento atual). Esta operação não é reversível, pelo que deve ter algum cuidado com o que faz –

eventualmente pode surgir alguma mensagem de erro, mas o importante é que verifique se o estado do certificado foi efetivamente alterado. Adicionalmente poderá ter que rever a política de gestão da sua CA, para que o efeito de revogação seja mais “eficiente” (pelo menos no contexto do exercício). Tem ainda a função CRL Monitor no ADSS que o ajuda a verificar o efeito da operação, ao nível do servidor. **Descreve a experiência no logbook, tendo o cuidado de indicar claramente as eventuais alterações e verificações que fez. Deve tentar verificar o efeito da revogação numa das aplicações que usou anteriormente.**

16. A última tarefa consiste em tentar estabelecer relações de confiança entre CAs dos colegas. **O que lhe é pedido é que descreva e teste o processo para conseguir implementar esse reconhecimento.**

Nota: quando criou a sua CA, foi conduzido para a criação de uma CA de raiz. Mas não teria que ser assim...