FICHA TRABALHO 2

MODALIDADE:	Aprendizagem +	Não aplicável	
CURSO:	Técnico/a Especialista em Gestão de Informação e Ciência dos Dados		
UFCD:	Segurança no desenvolvimento do software	CÓDIGO UFCD:	10795
FORMADOR/A:	Bruno Silva	DATA:	

OBJETIVOS

- Instalação e configuração ao mundo da criptografia e PGP (pretty good privacy)

Parte 1 – Criptografia

Criptografia é a disciplina que estuda os mecanismos de encriptação e desencriptação de informação.

Estes mecanismos recorrem basicamente a um ou mais algoritmos para codificação/descodificação da informação e uma ou mais chaves.

Pode estabelecer-se uma forte analogia entre mecanismos de encriptação e, por exemplo, um cofre-forte.

Apesar de saber como o mecanismo de abertura do cofre é construído (o algoritmo), o cofre não pode ser aberto sem se conhecer o segredo (combinação ou chave). Existe, no entanto, a possibilidade de tentar descobrir a combinação por métodos de força bruta, experimentando diversas combinações.

Resumindo, a criptografia é o processo de comunicação de informações num formato que pessoas não autorizadas não possam ler.

Somente uma pessoa autorizada e confiável com a chave secreta pode descriptografar os dados e aceder a informação original.



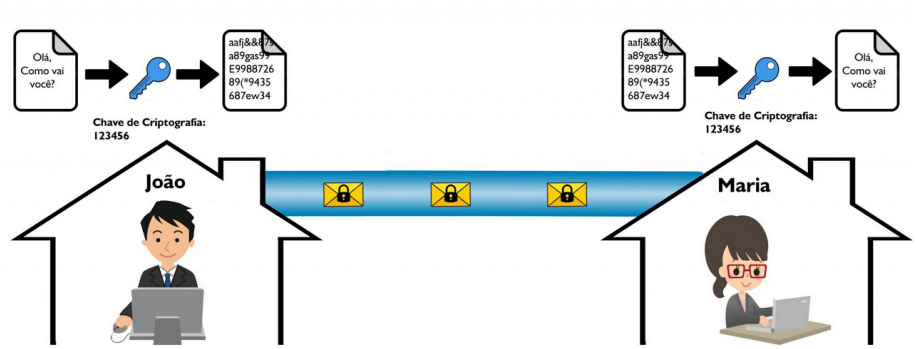
Atenção que: a criptografia em si não impede que alguém intercete os dados. Só pode impedir que uma pessoa não autorizada visualize ou aceda o conteúdo.

Parte 2 – Criptografia Simétrica Vs Assimétrica

Criptografia Simétrica

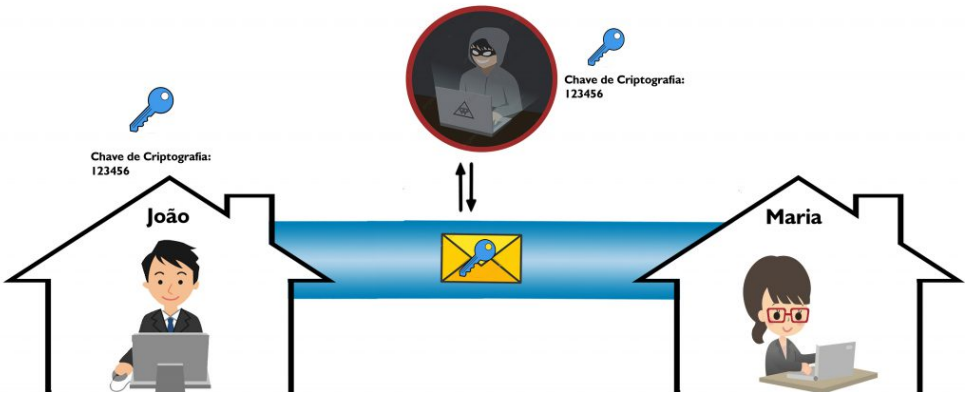
São criptografias baseadas em algoritmos que requerem uma única chave, que é usada tanto para as operações de codificação e descodificação da informação.

A chave, na prática, representa um segredo partilhado entre duas ou mais partes, que pode ser utilizada para manter um canal confidencial de informação.



O problema da chave simétrica está na distribuição da mesma. Caso: o João criou a chave e de entregar a chave para Maria. Como tal, a chave é enviada através da rede em texto puro.

Como a chave é enviada em texto puro, ela corre o risco de ser capturada no meio do caminho (possíveis espiões na rede), possibilitando assim que uma pessoa não autorizada tenha acesso a chave.



Criptografia Assimétrica

Surgiram após alguns anos de utilização dos algoritmos de chave simétrica e são criptografias baseadas em algoritmos que requerem 2 chaves: pública e privada. As duas partes desse par de chaves **estão matematicamente ligadas**.

Chave Pública

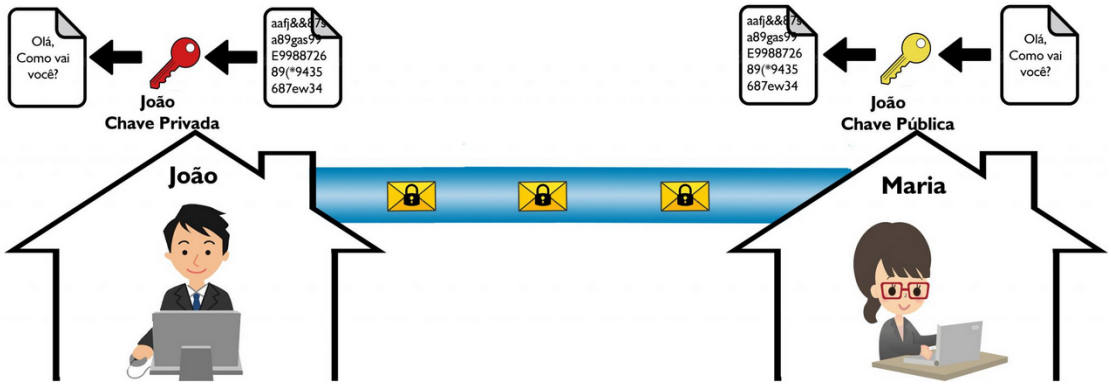
- A ***chave pública*** é utilizada, por exemplo, para **encriptar** uma mensagem para um destinatário e ter a certeza de que somente o destinatário terá acesso ao conteúdo original da mensagem ***ou*** para **verificar** uma assinatura digital pelo remetente.
- Pode ser publicada em **locais de partilha de chaves** para que os utilizadores a reconheçam.

Chave Privada

- Já a ***chave privada*** é ***utilizada para a operação oposta***, ou seja, para ***desencriptar*** uma informação previamente criptografada (proveniente de um remetente e obter o conteúdo original da mensagem) ou para ***assinar digitalmente*** uma mensagem antes de a enviar ao destinatário.
- A chave privada **deve ser mantida em segredo** e eventualmente protegida com mecanismos de palavra-chave para garantir a sua segurança.



Exemplo mais concreto:



A ***chave pública*** é enviada em texto puro pela rede, assim como a chave simétrica. Mesmo que a chave pública do João seja capturada no caminho, a única maneira de descriptografar os dados criptografados pela chave pública do João, é com a ***chave privada***. Como tal, o João nunca deverá distribuir sua chave privada.

E se o João quiser enviar dados criptografados para a Maria?

Bem, nesse caso a Maria deverá gerar o par de chaves (pública e privada), tal e qual como foi feito pelo João. Assim ambos podem trocar dados criptografados sem problemas.

Parte 3 – Software pgp4Win

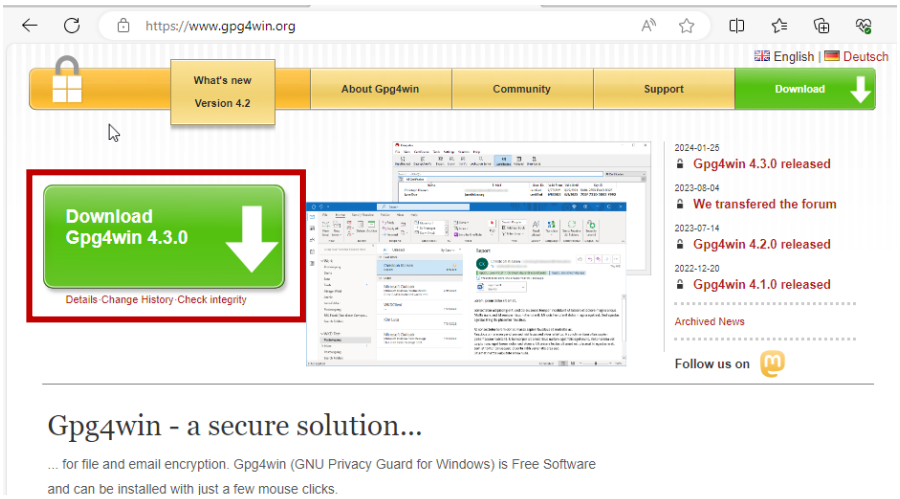
O software Gpg4Win é uma aplicação com programas para criptografia de e-mail e ficheiros que utiliza o GnuPG, software de código aberto que segue o padrão OpenPGP.

O pacote inclui os seguintes programas para Windows:

- ***GnuPG***: o núcleo da aplicação, responsável pela criptografia em si;
- ***Okular (GnuPG)***: para assinar documentos pdf;
- ***Kleopatra***: vai ficar presente na bandeja do sistema (ao lado do relógio). Inclui gerenciador de chaves e teclas de atalho configuráveis;
- ***GpgOL***: um plugin (suplemento) para criptografar e-mails no Microsoft Outlook;
- ***GpgEx***: adiciona ao menu do shell (aceder ao clicar com o botão direito do rato num arquivo do Windows), funções de criptografar, assinar, etc...

Passos de instalação:

1. Aceder a página oficial da aplicação https://www.gpg4win.org e clicar no botão "Download Gpg4win ...":

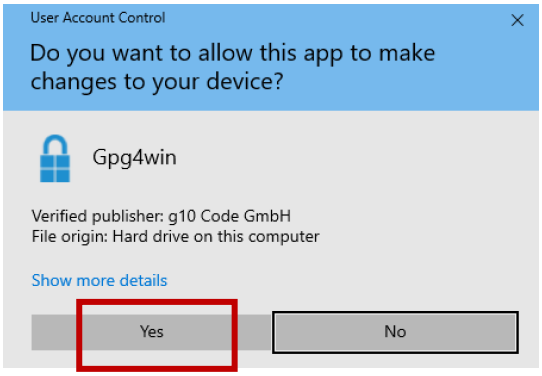


2. Carregar no botão clicar no botão "Download":

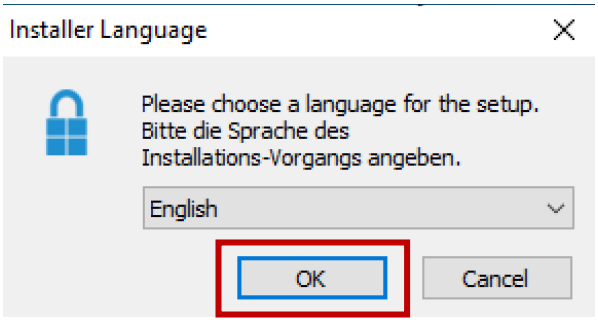




3. Executar o programa e confirmar a operação:

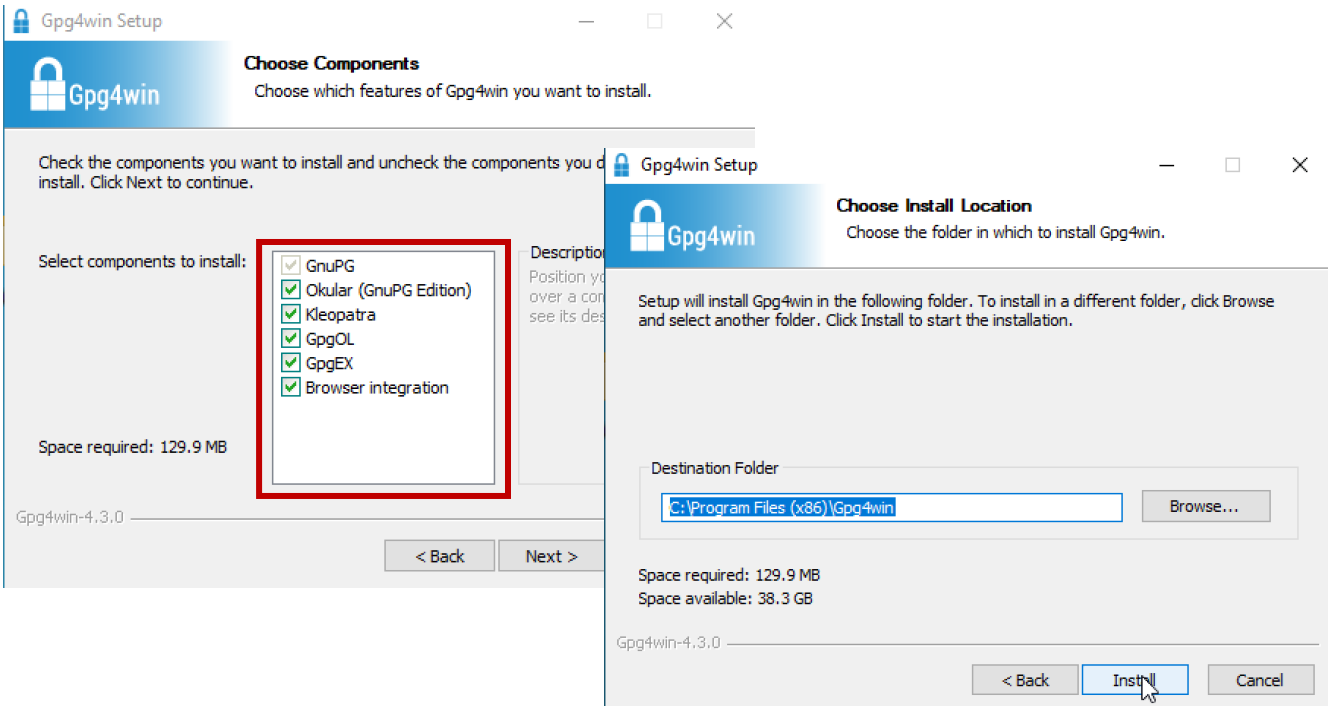


4. Selecionar a linguagem da instalação:

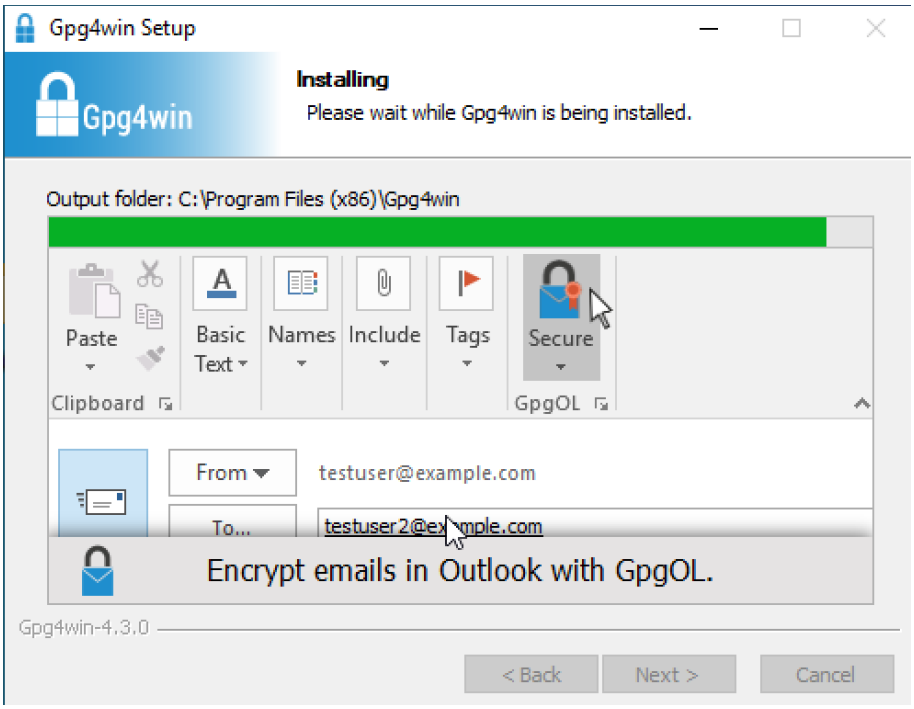




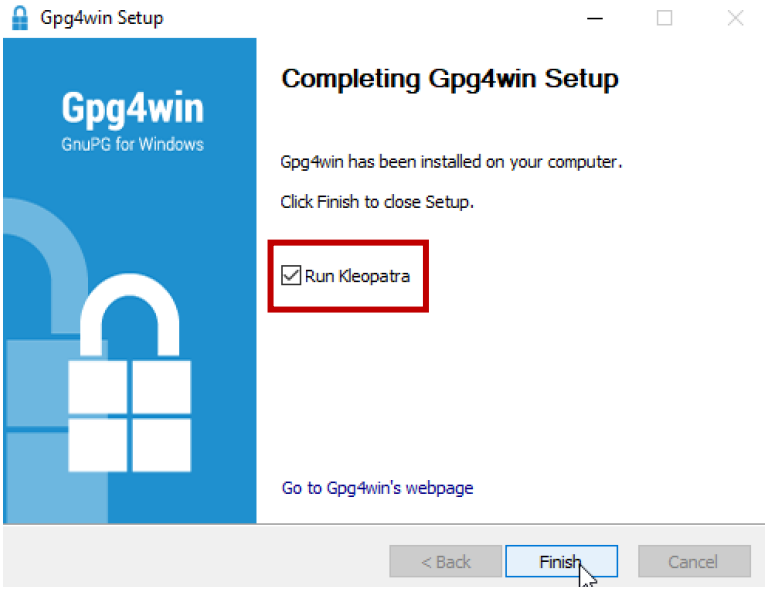
5. Confirmar a instalação dos componentes e a localização no computador:



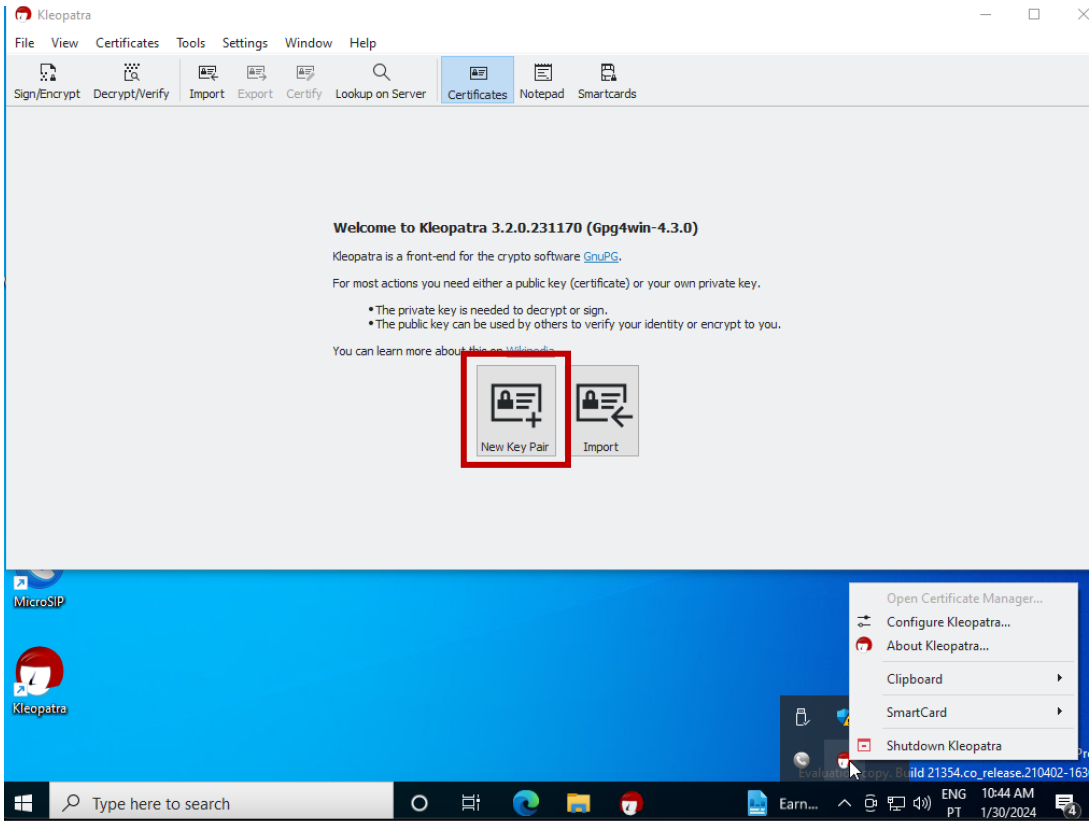
6. Este vai instalar todos os componentes e devem aguardar pela finalização da instalação:



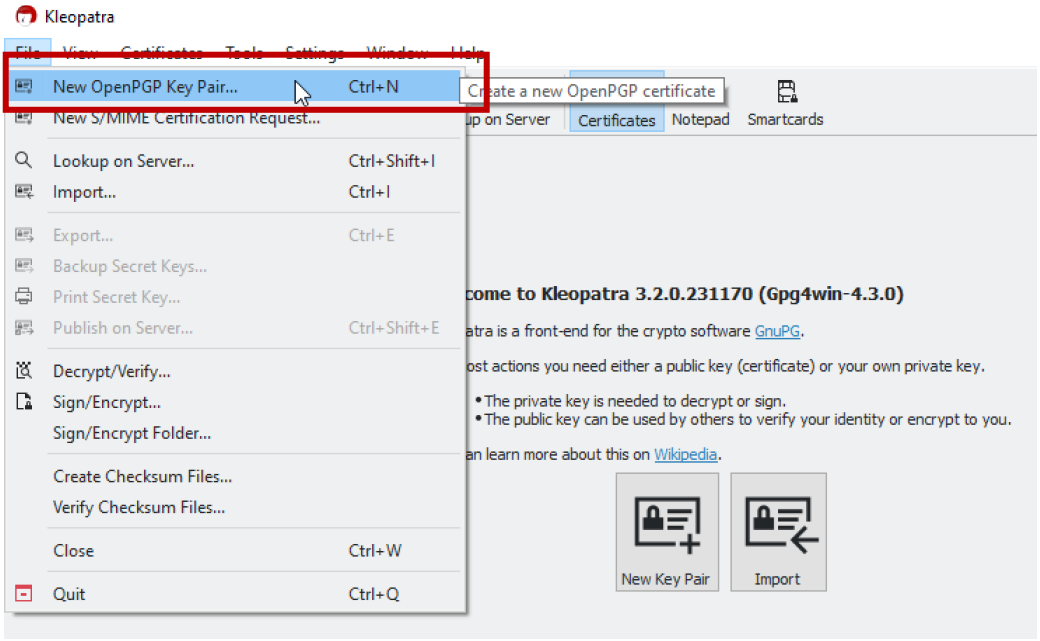
7. No final, vamos verificar se este vai executar o programa Kleopatra:



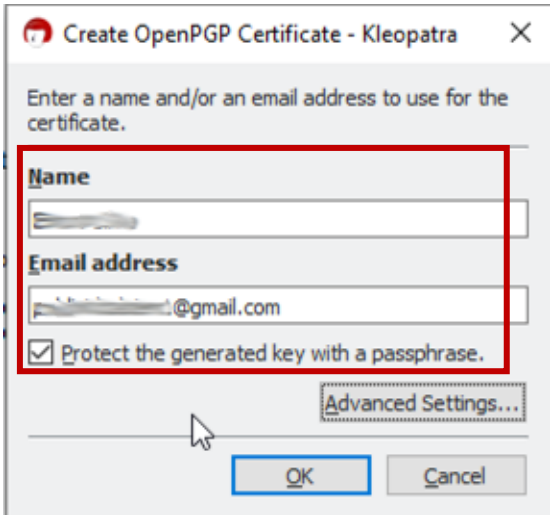
8. Ao abrir o programa Kleopatra, vamos começar por gerar as chaves públicas e privadas. Para tal pode clicar no botão no centro do programa "New Key Pair":



Ou eventualmente, ir ao Ficheiro → New OpenPGP Key Pair:

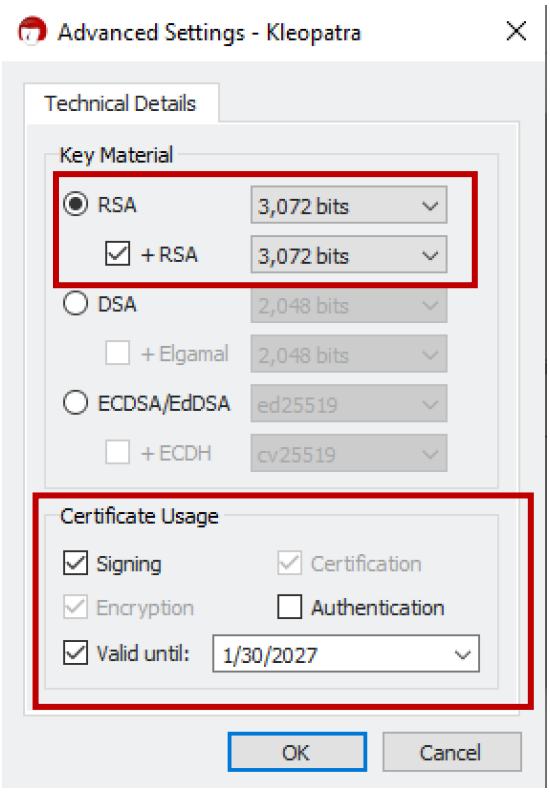


9. Indicar os dados do utilizador e um email:

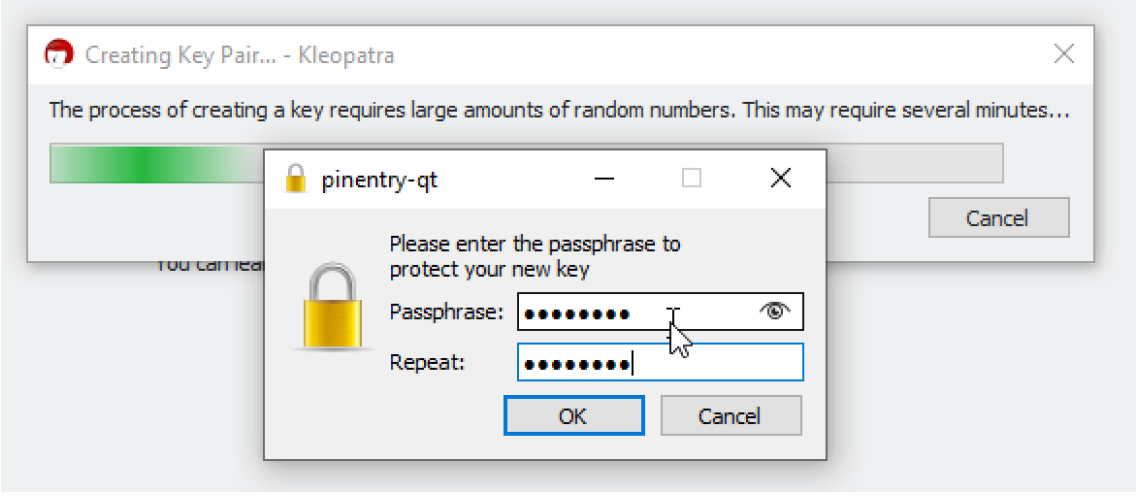


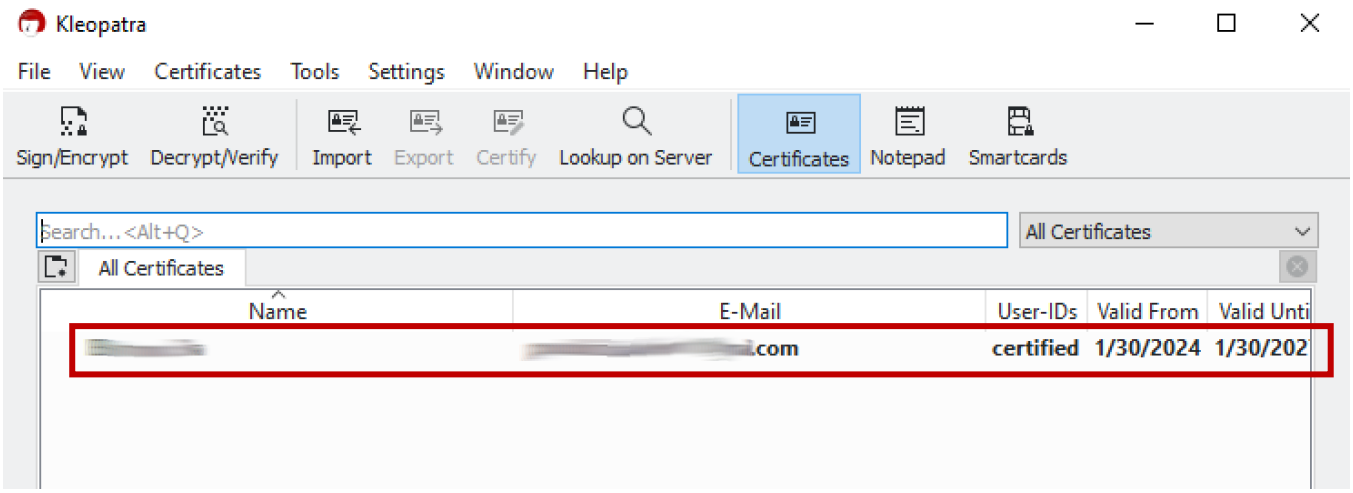
10. De seguida clique no botão "Advanced Settings...", onde poderá selecionar a encriptação com o ECDSA/EdDSA. ***O problema desta encriptação*** é que utiliza uma criptografia de assinaturas baseadas nas curvas elípticas (funções matemáticas de álgebra linear) e ***nem todos os programas suportam esse tipo de encriptação***.

Para tal, vamos utilizar o ***modelo padrão do RSA*** que já contem uma encriptação até 4096 bits (mas para este caso ***vamos utilizar 3072 bits***):



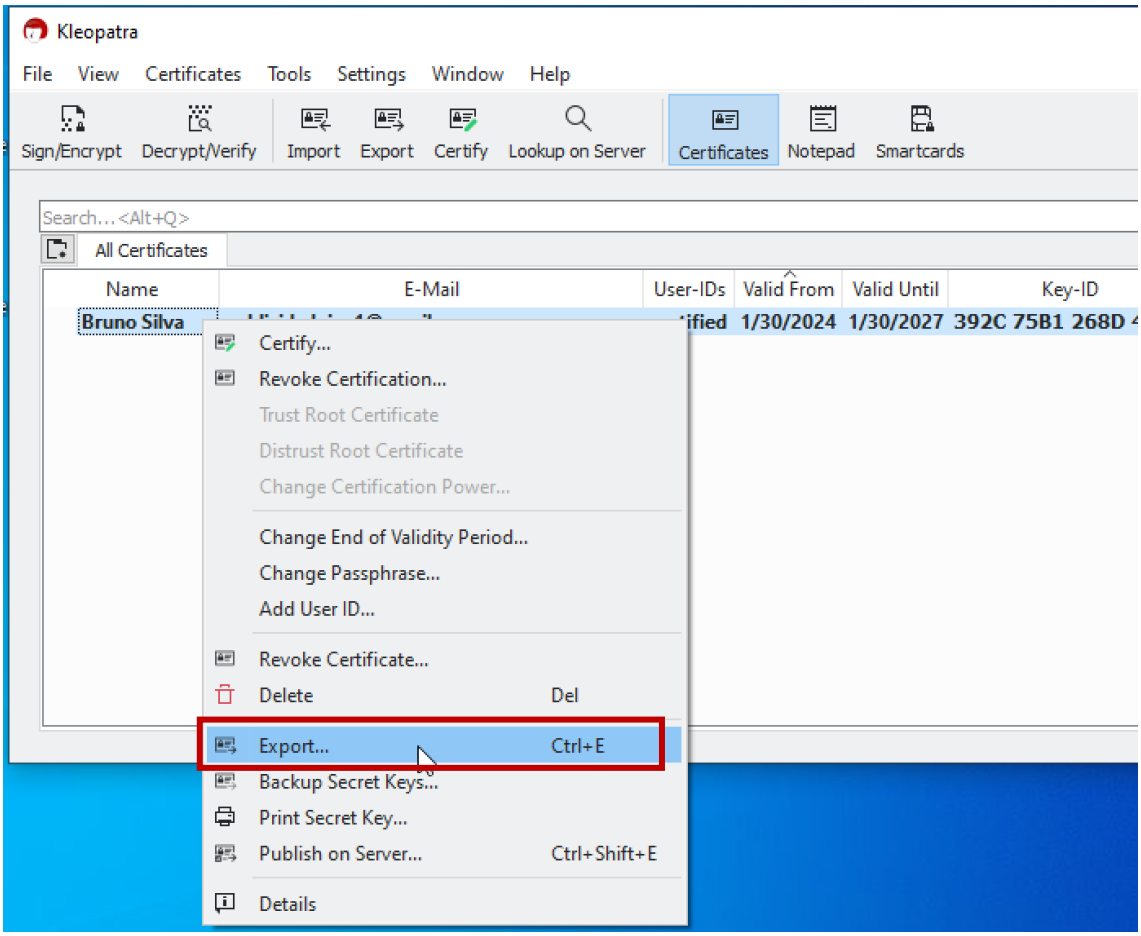
11. Colocar password de proteção e confirmar a mesma e verificar a criação do processo:



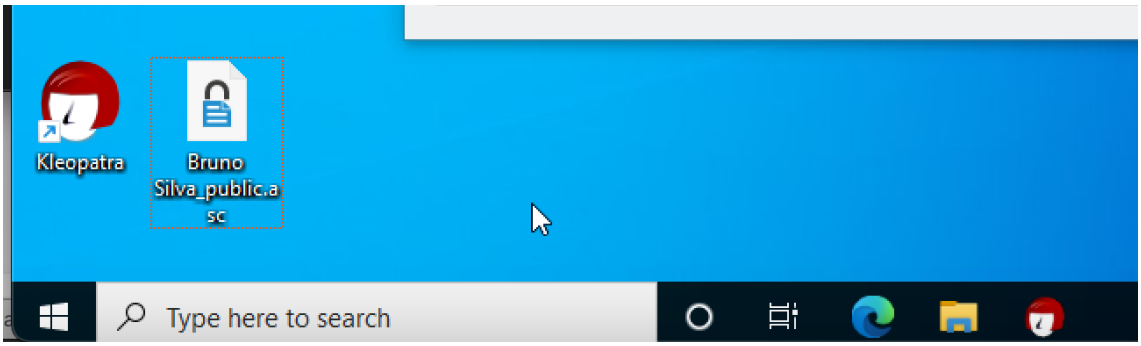

Kleopatra
File View Certificates Tools Settings Window Help
Sign/Encrypt
Decrypt/Verify
Import
Export
Certify
Lookup on Server
Certificates
Notepad
Smartcards
Search... <Alt+Q>
All Certificates
All Certificates
Name
E-Mail
User-IDs
Valid From
Valid Unti
[redacted]
[redacted].com
certified
1/30/2024
1/30/202

Parte 4 – Exportar Chave Pública e Privada

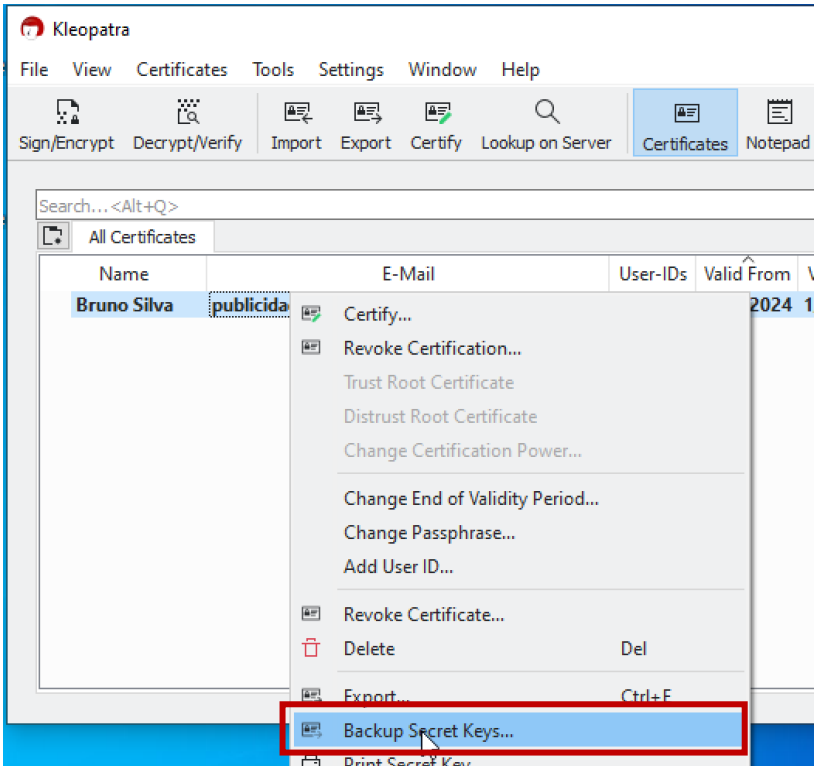
1. Para exportar a chave pública, vamos carregar com o lado direito do rato em cima do certificado que pretendemos exportar e selecionar a opção “Export”:



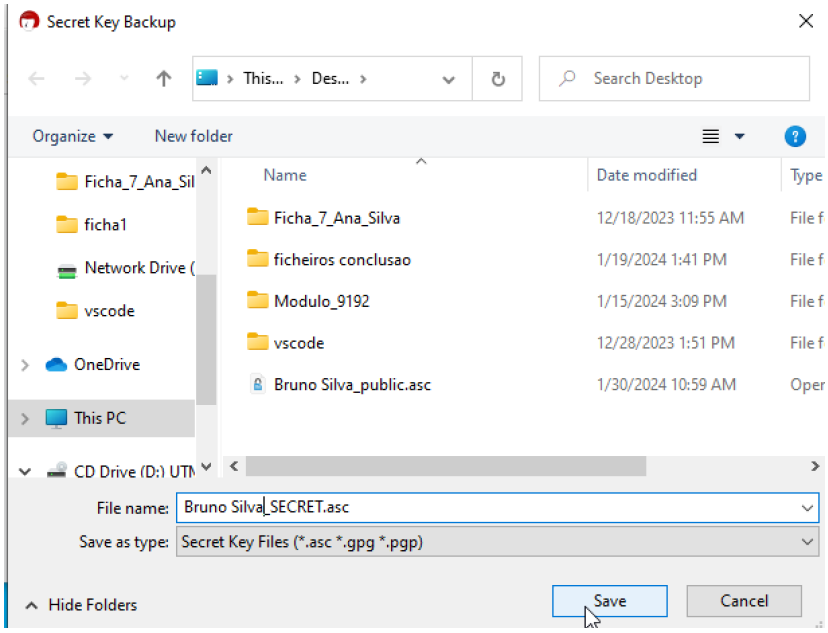
E de indicar a localização onde deseja guardar a chave pública (neste caso no ambiente de trabalho):



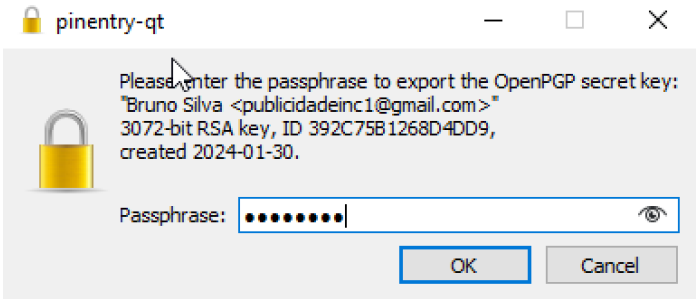
2. Para exportar a chave privada, vamos carregar com o lado direito do rato em cima do certificado que pretendemos exportar e selecionar a opção “Backup Secret Keys...”:

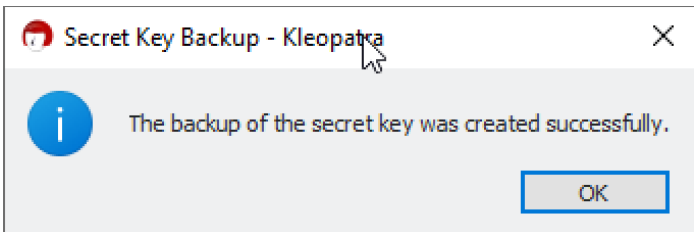


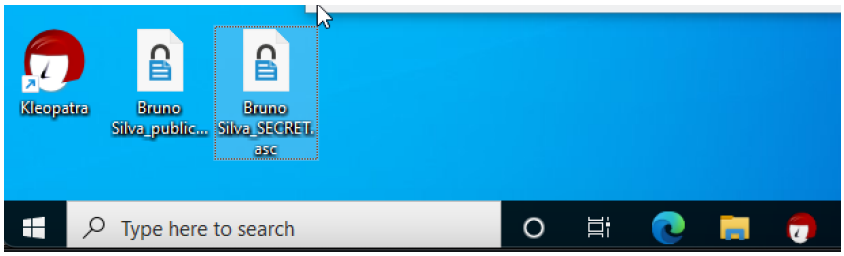
E de indicar a localização onde deseja guardar a chave privada (neste caso no ambiente de trabalho):



3. Como estamos a exportar a chave privada, temos de indicar a palavra-passe que definimos anteriormente (para confirmar a operação):

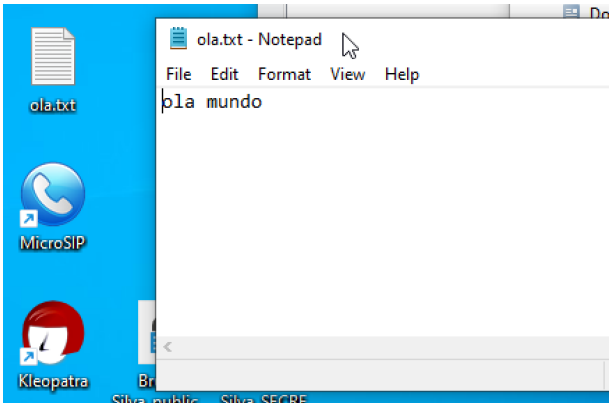




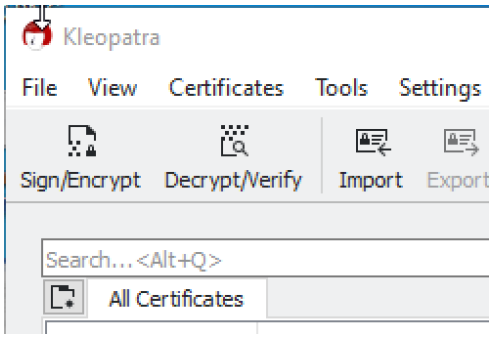


Parte 5 – Assinar ficheiros (para verificar a integridade da informação)

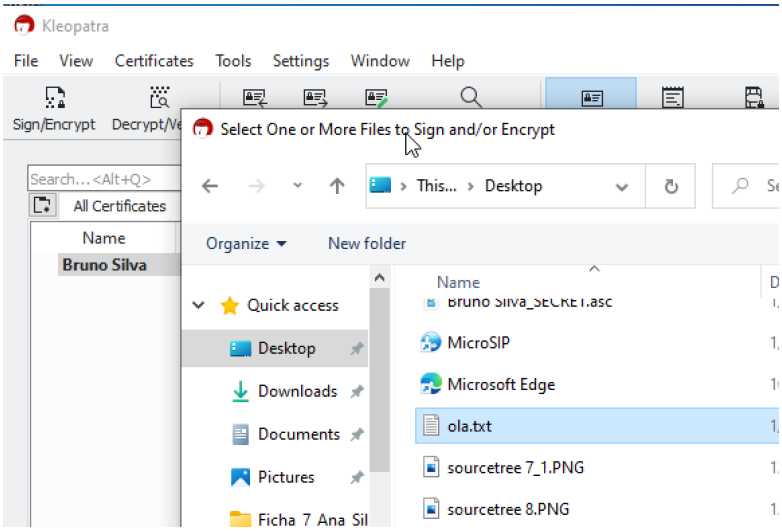
1. Crie um documento no ambiente de trabalho com alguma informação no seu conteúdo:



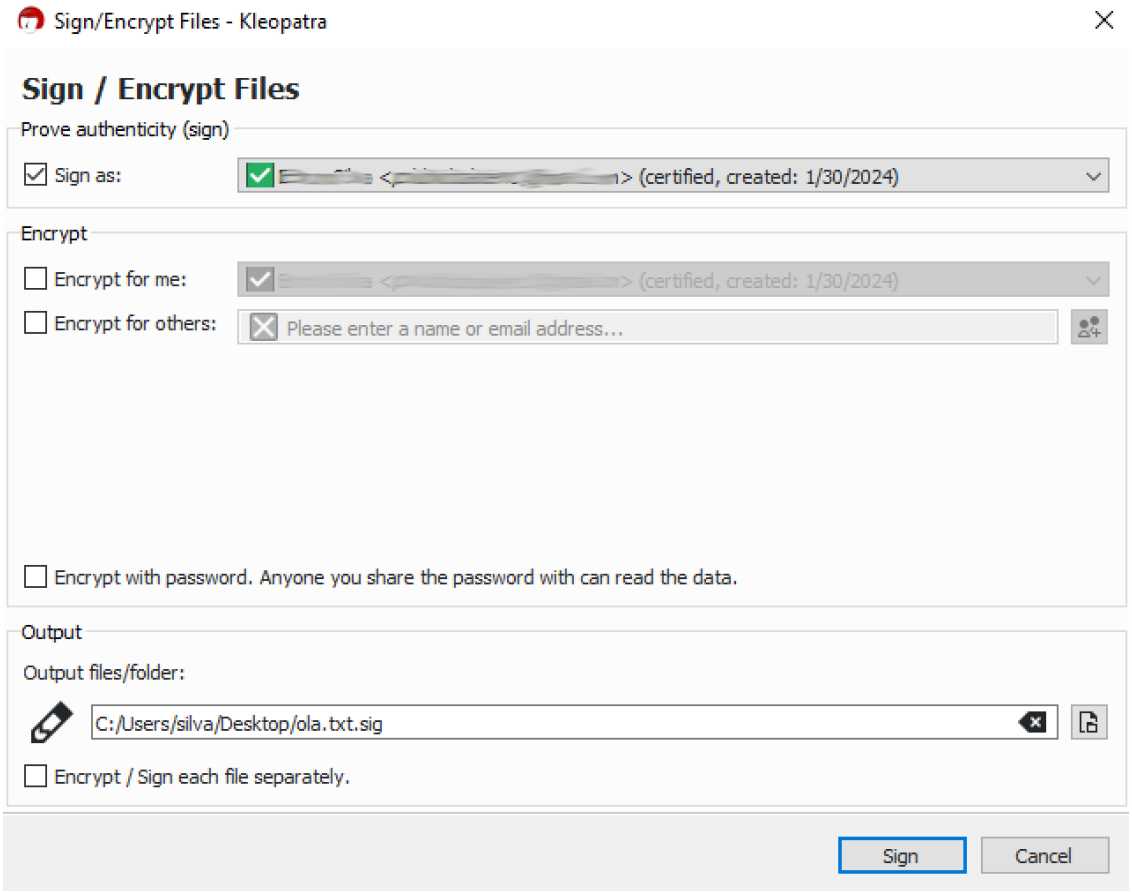
2. De seguida, vamos assinar o documento para manter a integridade da informação. Como tal, Clique na opção "Sign/encript" (pois este botão tem duas funcionalidades):



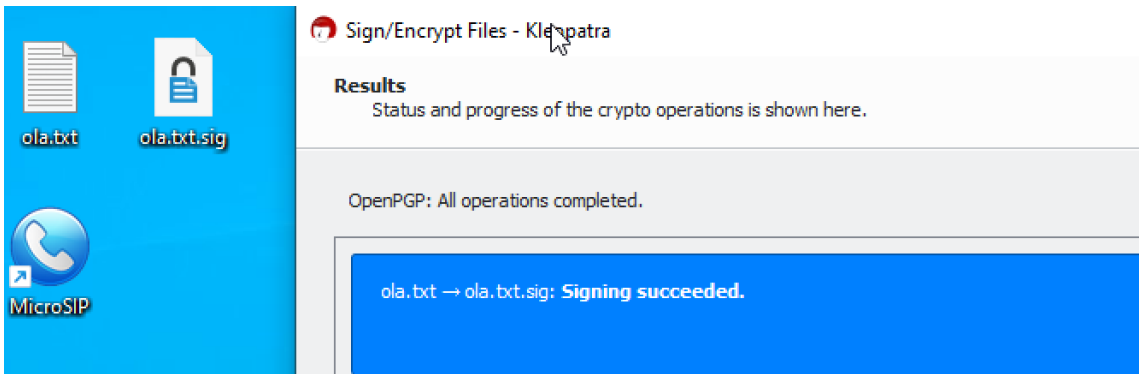
3. Selecione o ficheiro que acabou de criar:



4. Selecionar apenas a opção “Sign as” (normalmente já vem por defeito) e clique no botão “Sign”:



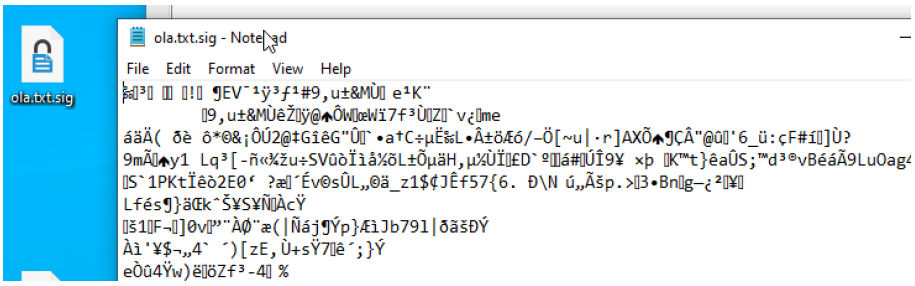
5. Verificar se o ficheiro foi assinado com sucesso:



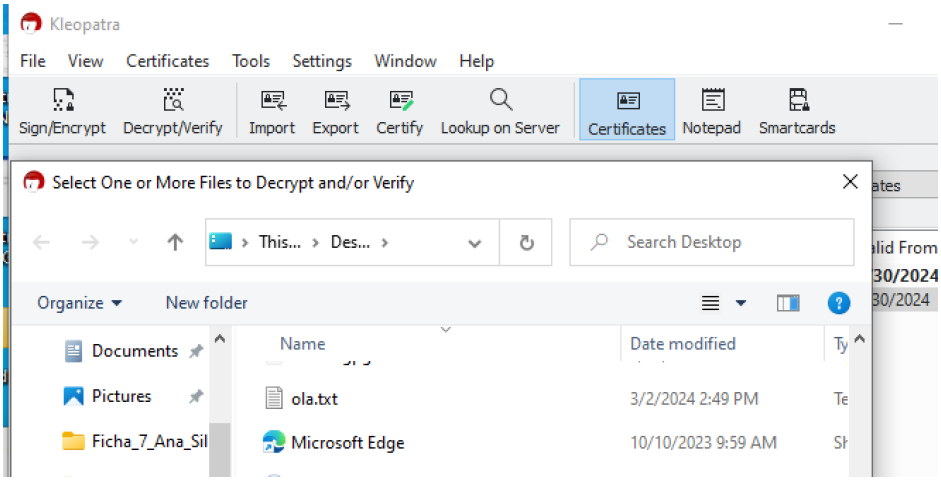
Parte 6 – Assinar ficheiros (para verificar a integridade da informação)

Verificação do ficheiro (sem alteração do conteúdo no ficheiro)

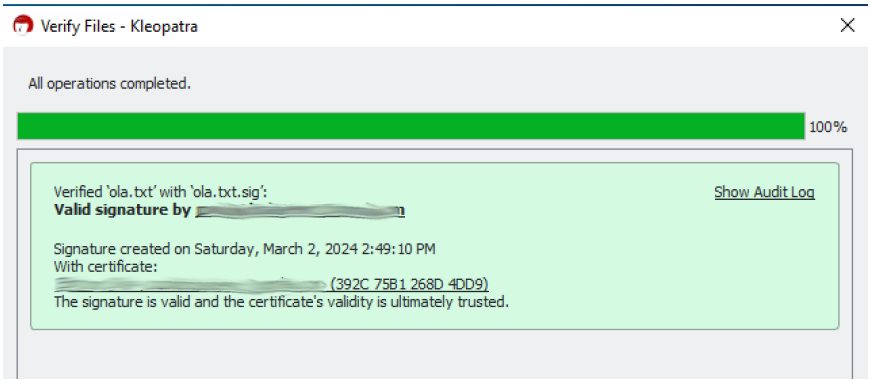
1. Quando abrir o ficheiro da assinatura, este terá a informação de forma criptografada:



2. Para confirmar se a integridade do ficheiro foi alterada, vamos ao programa Kleopatra e selecionar as opções “Decrypt/Verify” (pois este botão tem duas funcionalidades) e indicar a localização do ficheiro que foi assinado:

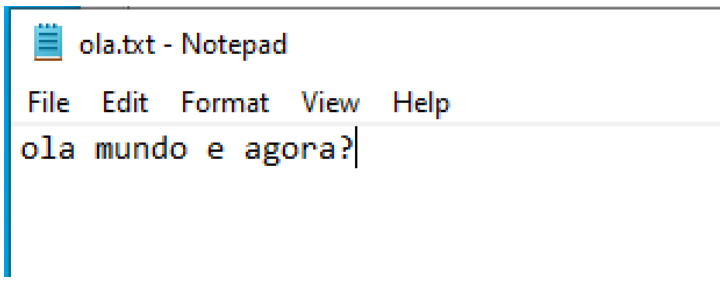


3. Este vai verificar se está tudo em condições e irá dar o resultado:

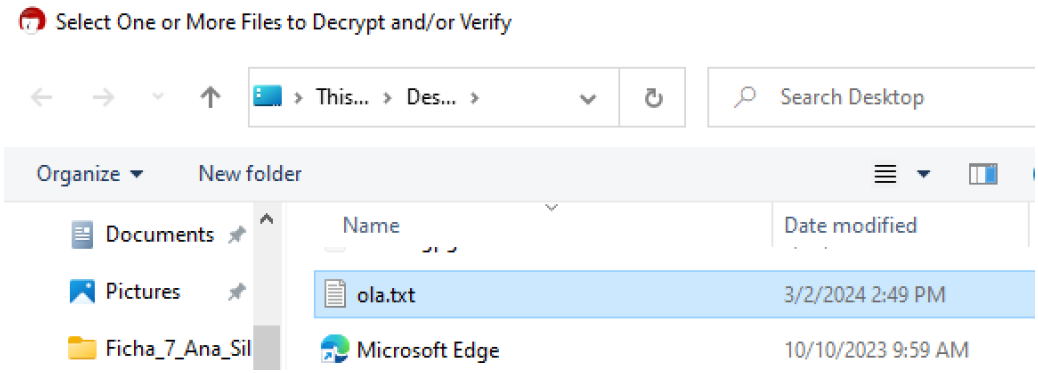


Verificar do ficheiro (mas também <u>com alteração</u> da informação no ficheiro)

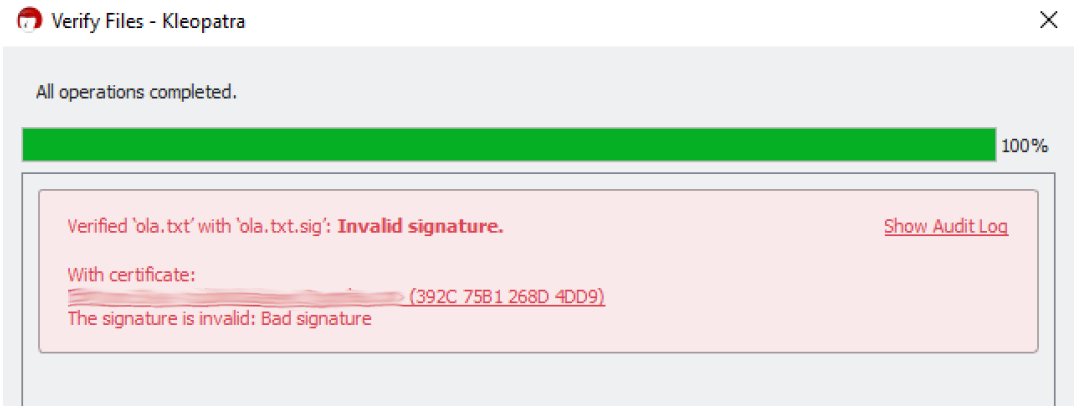
1. Abra o ficheiro que foi assinado, e coloque informação:



2. Para confirmar se a integridade do ficheiro foi alterada, vamos ao programa Kleopatra e selecionar as opções “Decrypt/Verify” (pois este botão tem duas funcionalidades) e indicar a localização do ficheiro que foi assinado:



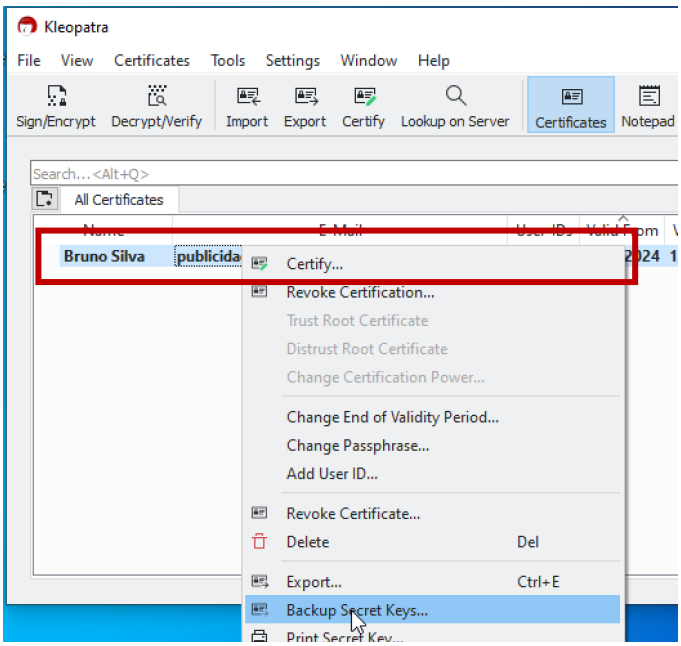
3. Este vai verificar se está tudo em condições e irá dar o resultado (do qual irá falhar, pois a integridade da informação foi alterada):



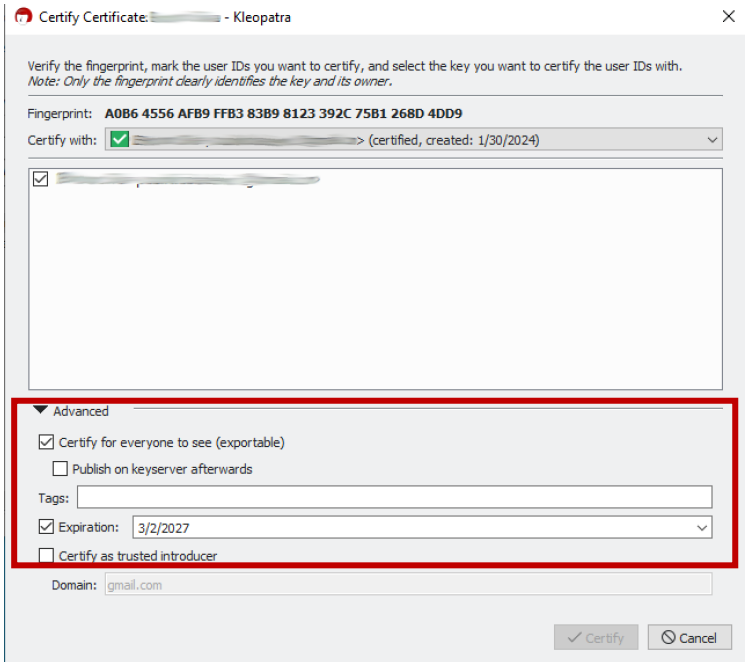
Parte 7 – Certificar e publicar chave pública no servidor Kleopatra

Podemos certificar e ***publicar*** a nossa ***chave pública no servidor Kleopatra***, para que todas as pessoas possam ***pesquisar o seu endereço o nome de utilizador na pesquisa do servidor Kleopatra*** e importar a chave pública que foi disponibilizada;

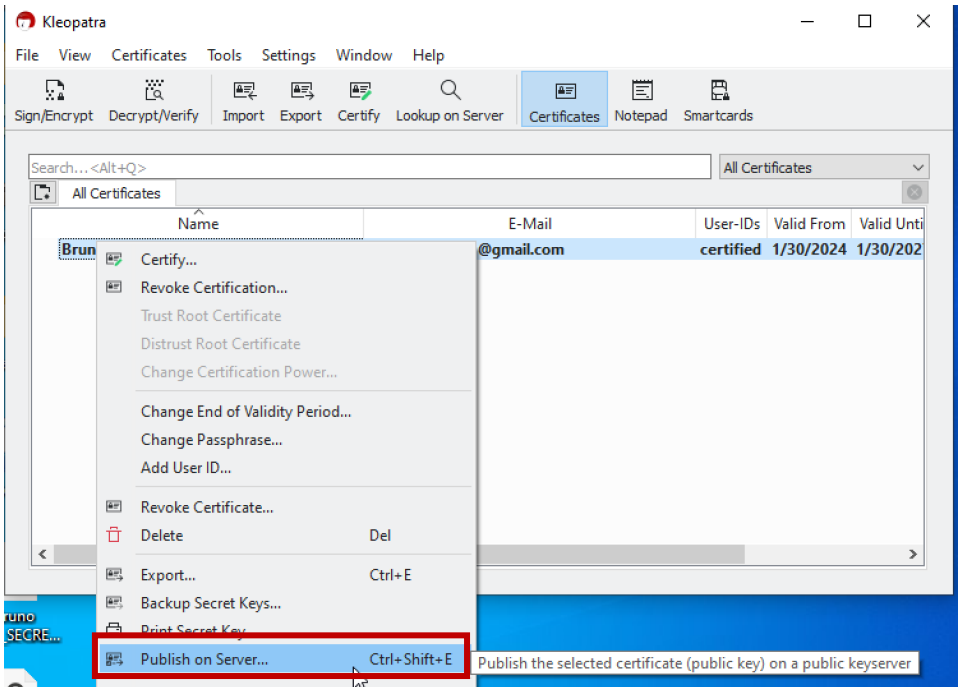
1 – Para certificar, basta clicar na sua chave e com o lado direito do rato, selecionar a opção "Certify...";



2 – Colocar um limite na certificação e permitir que todos possam pesquisar pela chave:



3 **–** Depois de certificar, vamos colocar no servidor da Kleopatra:



E aceitar as condições enunciadas:

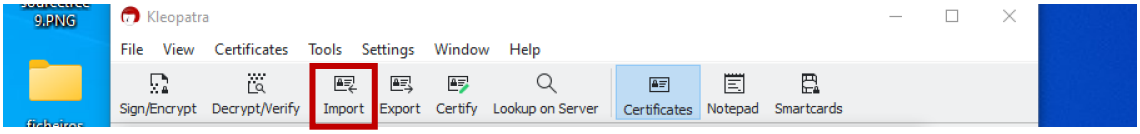


Parte 8 – Assinar e encriptar ficheiro (com autorização de assinaturas)

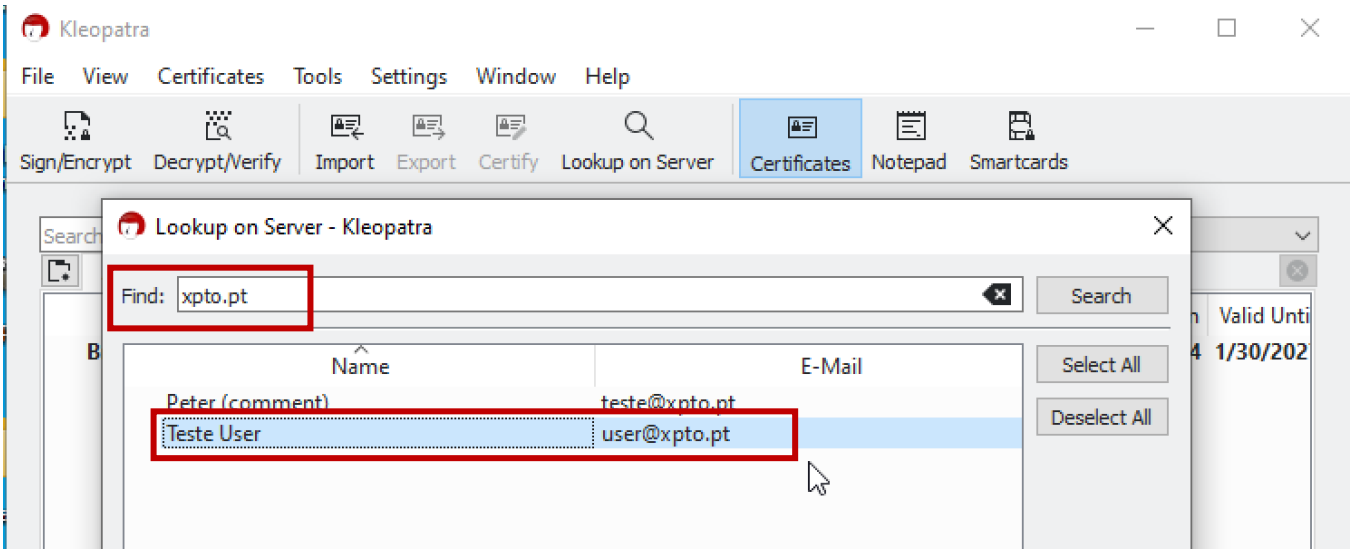
Também podemos utilizar outra funcionalidade de proteção de informação, mais especificamente, encriptar o(s) ficheiro(s) para pessoas autorizadas (todos os outros não vão conseguir ver a informação). Para tal, precisamos de importar as chaves públicas de outras pessoas no nosso programa.

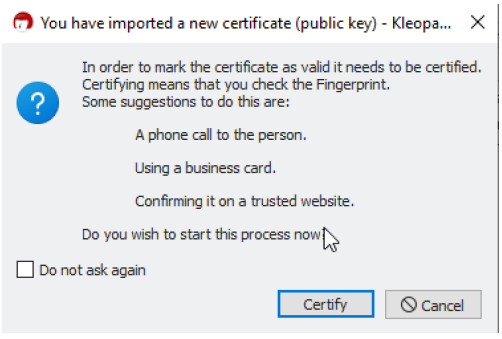
Para fazer isso temos duas formas possíveis:

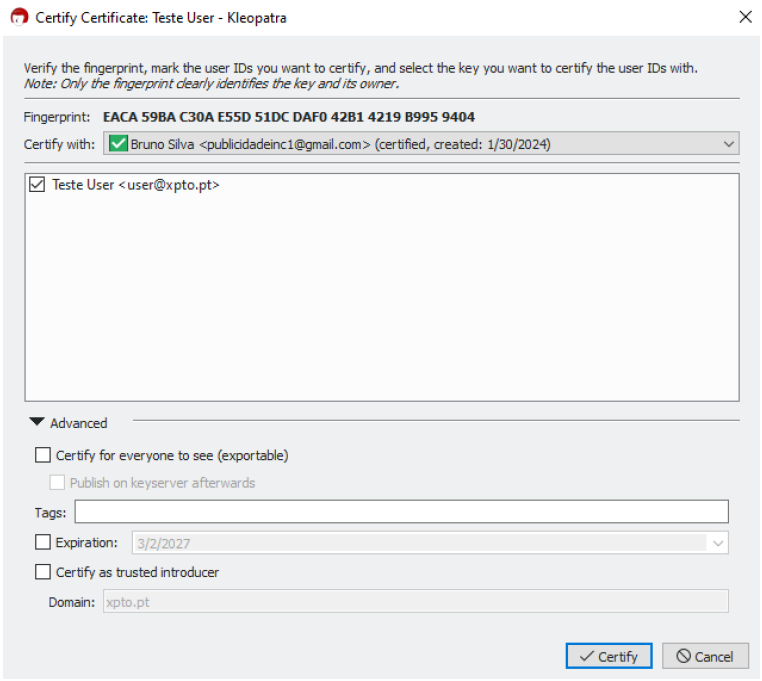
1 – ***Importar uma chave pública*** que tenha ***sido enviado por uma pessoa de confiança e certificar***;



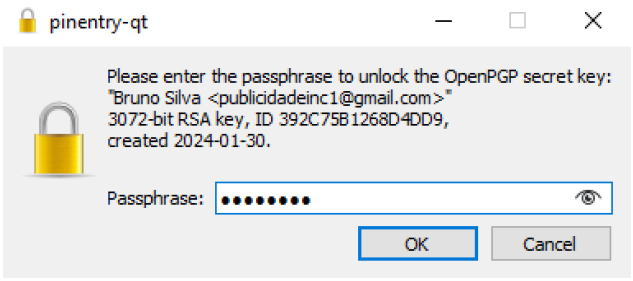
2 – ***Se a chave pública estiver no servidor Kleopatra***, pode ***pesquisar o endereço de email ou nome de utilizador*** na pesquisa do servidor Kleopatra e importar a chave pública que foi disponibilizada;

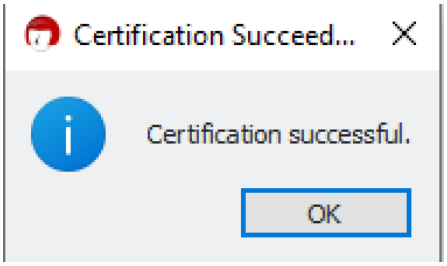






Para confirmar a importação, deve inserir a password da sua chave privada para confirmar que fomos nós o autor da importação:





3 – Para encriptar ficheiros para outras pessoas, deve selecionar o campo Encrypt for others e selecionar quem pretende enviar a informação:

FICHA TRABALHO 2

