Manual do utilizador da aplicação

Informações de interesse

A. Objectivos

- Promover a troca de informações de forma anónima e segura.
- Implementação da criptografia na transferência de ficheiros na Intranet.
- Criar uma plataforma alternativa para a partilha de ficheiros entre estudantes da UBI.

B. Quem somos nós?

Somos um grupo de alunos da Universidade da Beira Interior, do curso de Informática Web, e temos também um elemento da Engenharia Informática. Estamos a fazer a cadeira de Segurança Informática e este é o nosso projecto final.

C. Dados Técnicos

No código fornecido, três algoritmos de criptografia são utilizados: RSA, AES e HMAC. Explicando brevemente cada um deles e como eles são utilizados:

C.1 RSA (Rivest-Shamir-Adleman):

- RSA é um algoritmo de criptografia assimétrica amplamente utilizado para criptografar e descriptografar dados.
- Ele envolve o uso de um par de chaves: uma chave pública para criptografar os dados e uma chave privada correspondente para descriptografá-los.
- No código, a função `generateRSAKeys()` é usada para gerar um novo par de chaves pública e privada.

C.2 AES (Advanced Encryption Standard):

- AES é um algoritmo de criptografia simétrica amplamente adotado para criptografar e descriptografar dados.
- Diferente do RSA, o AES utiliza a mesma chave para criptografar e descriptografar os dados.
- No código, a função `encryptAES()` é usada para criptografar os dados com uma chave AES e `decryptAES()` é usada para descriptografá-los.

C.3 HMAC (Hash-based Message Authentication Code):

- HMAC é um algoritmo usado para verificar a integridade e autenticidade de uma mensagem.
- Ele envolve o uso de uma função hash (como SHA-256) combinada com uma chave secreta.
- No código, a função `generateHMAC()` é utilizada para gerar um código HMAC para uma mensagem específica com uma chave secreta fornecida.

Esses três algoritmos trabalham em conjunto para fornecer criptografia, autenticação e integridade dos dados transmitidos. O RSA é usado para troca de chaves e criptografia dos dados, o AES é utilizado para criptografar os dados em si, e o HMAC é empregado para verificar se os dados não foram alterados durante a transmissão.

D. Questões Jurídicas

D.1 No que diz respeito à utilização da aplicação, não somos responsáveis pelos conteúdos partilhados ou descarregados.

D.2 No caso de um ataque de hackers em que a base de dados seja comprometida, a segurança dos ficheiros é garantida pela encriptação e, como não guardamos chaves privadas, o atacante não conseguirá desencriptar. Não garantimos a protecção de ficheiros não encriptados.

D.2.1 No entanto, um atacante pode encriptar conteúdos maliciosos e enviá-los para si. Por isso, certifique-se de que dispõe de mecanismos externos para confirmar os envios que recebe (não somos responsáveis por este facto).

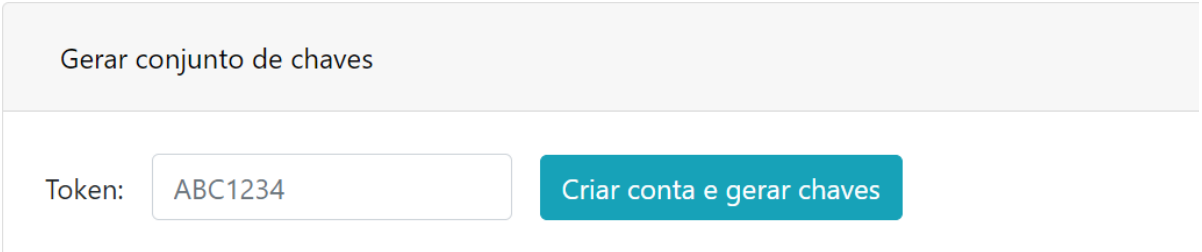
Plataforma e formas de deslocação entre secções:

Visão geral: Esta será a vista quando iniciar sessão pela primeira vez. Poderá haver versões diferentes devido a actualizações, mas a estrutura geral será mantida.

Como pode ver na imagem, existem diferentes categorias, que explicaremos mais adiante. Para entrar em cada uma das secções, basta carregar no texto do collapse e será apresentada uma janela de forma dinâmica.

Devido ao tamanho do browser, estas janelas podem não mostrar todas as informações, pelo que terá de utilizar o scroll do rato para visualizar as informações.

<u>Geração de chaves e token</u>

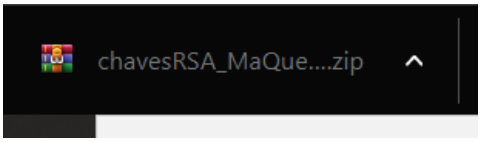


A. Passos: De forma intuitiva, basta inserir o token como nome de usuário (ex. MaQuer84) para que os outros utilizadores possam enviar ficheiros encriptados ou não encriptados para o token gerado.

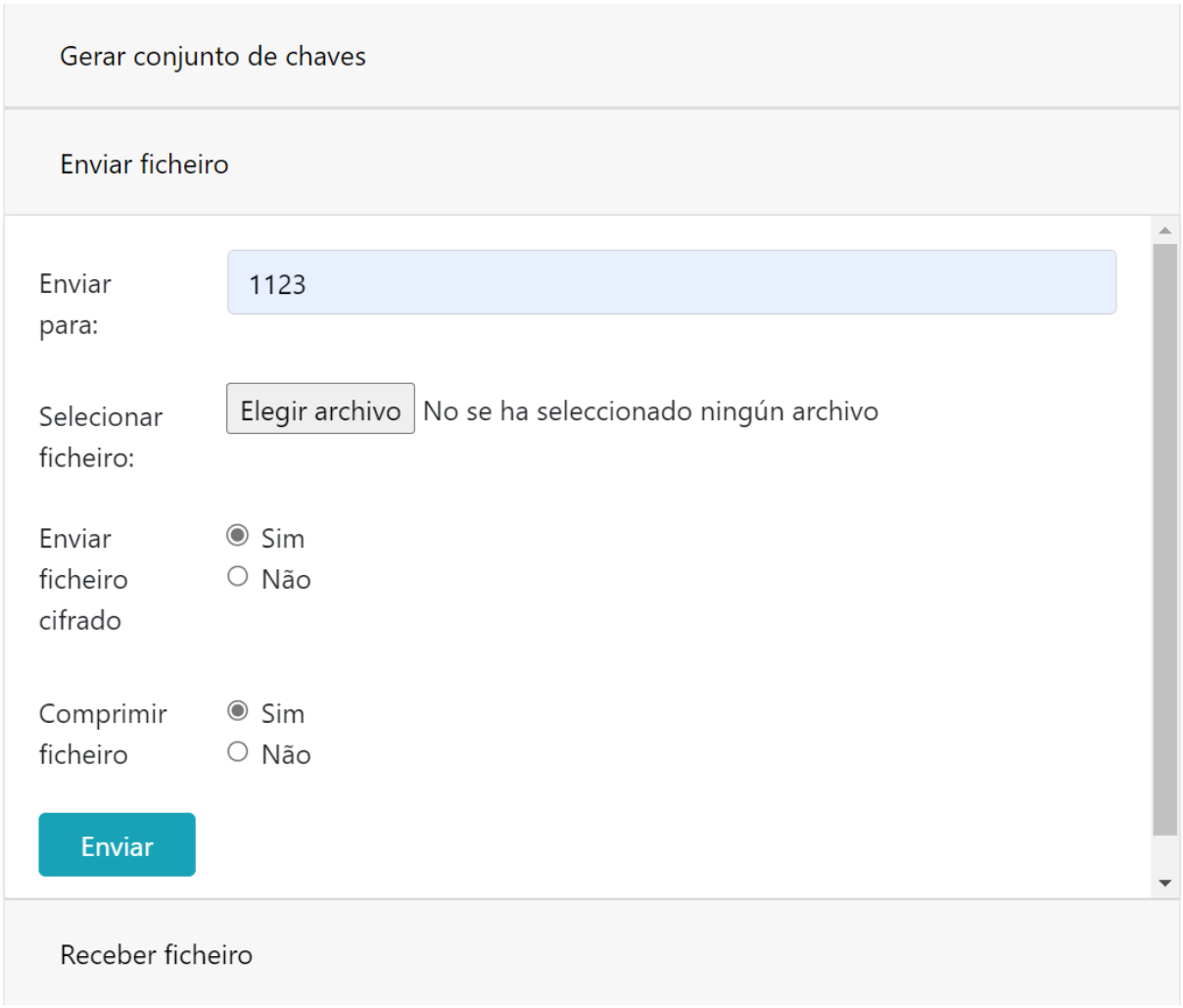
B. Em seguida, clique no botão "Criar conta e gerar chaves", o que criará automaticamente o token e descarregará as chaves privada e pública num ficheiro .zip. É necessário

guardar a chave privada para desencriptar e receber ficheiros.

C. Aparecerá no seu browser ou na pasta Downloads:

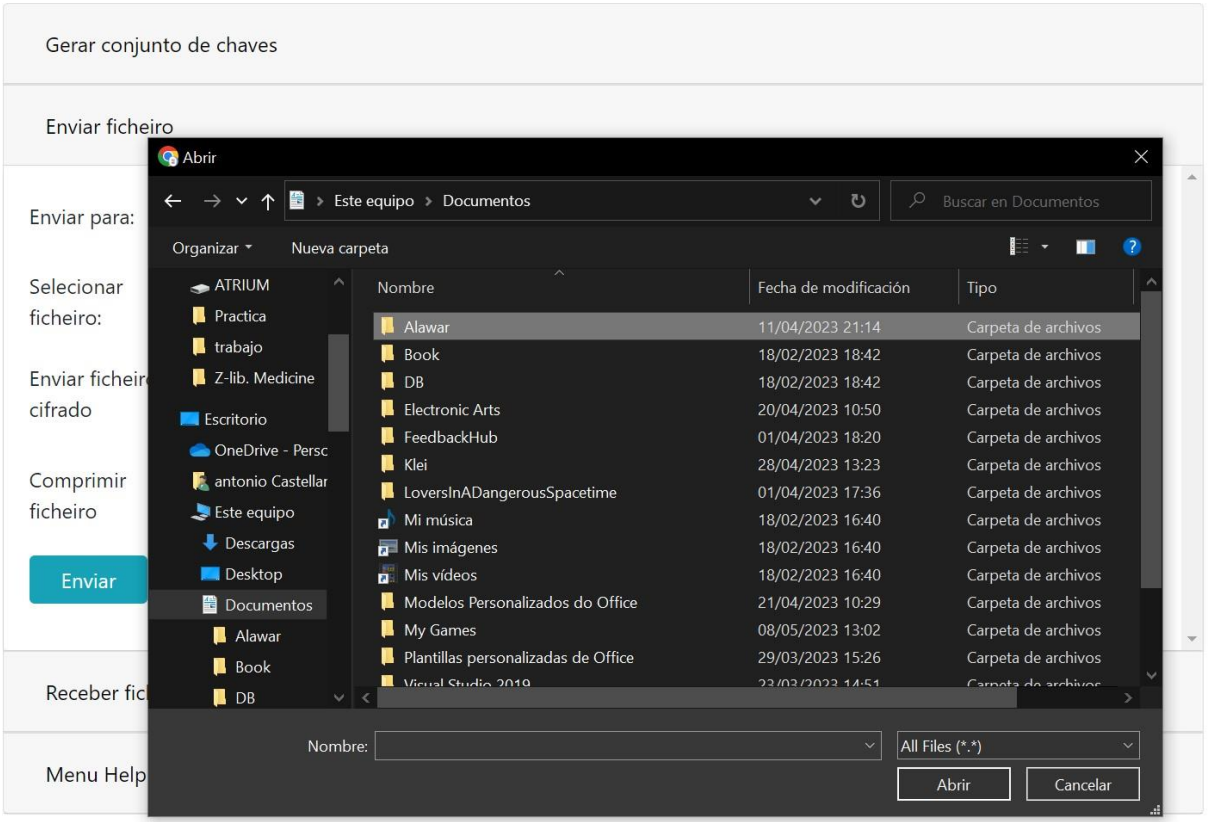


Enviar ficheiros



A. Para enviar um ficheiro, é necessário introduzir o token da pessoa a quem o quer enviar, pois, caso o ficheiro seja cifrado, será utilizado a chave pública do token de destino. Além disso, o responsável pelo token de destino poderá fazer uma listagem dos ficheiros que foram enviado para ele.

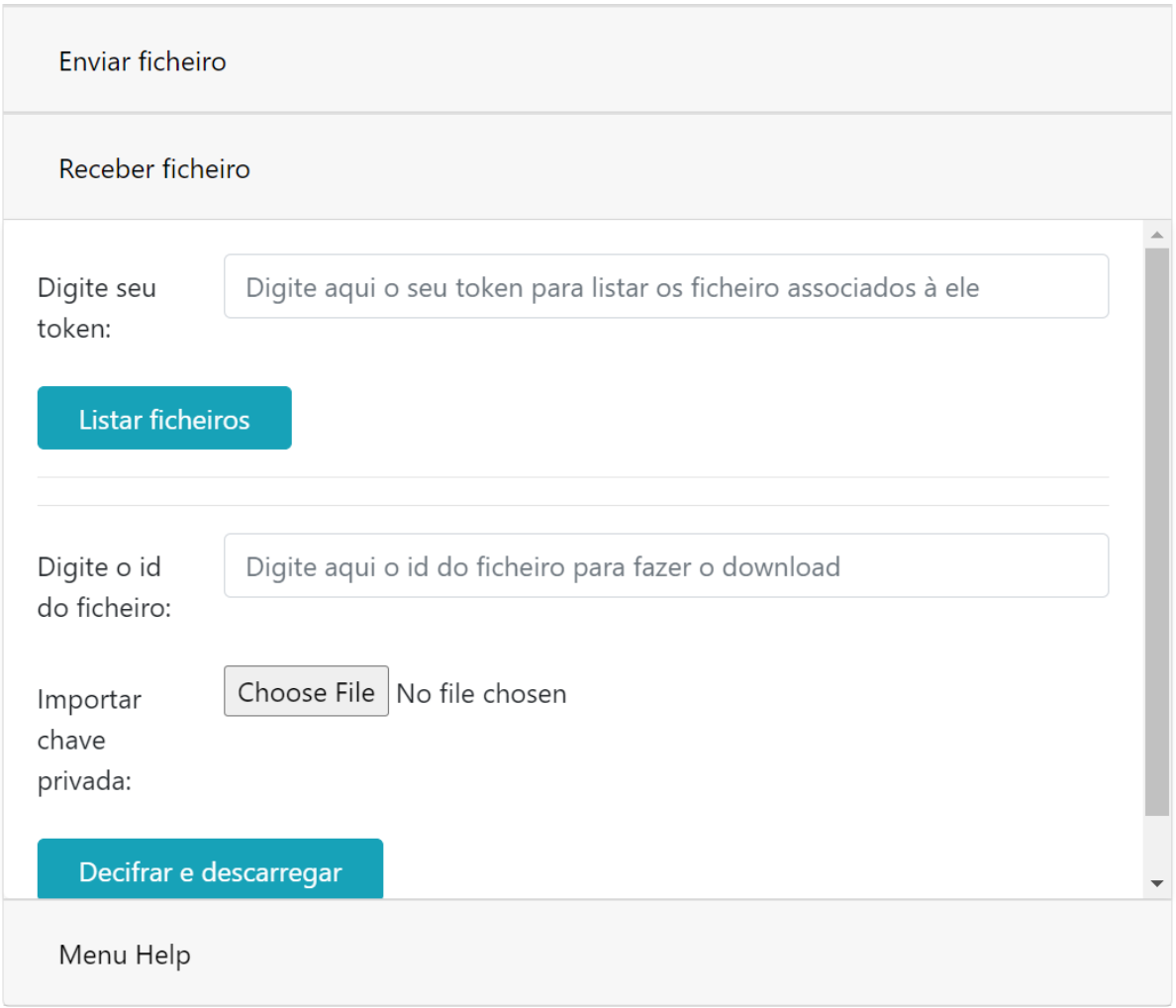
B. Em seguida, o botão "Choose File" mostra uma janela para seleccionar o ficheiro que se pretende enviar, como na seguinte imagem:



C. Depois de selecionar o ficheiro, pode-se escolher nas opções se o quer encriptar e/ou comprimir.

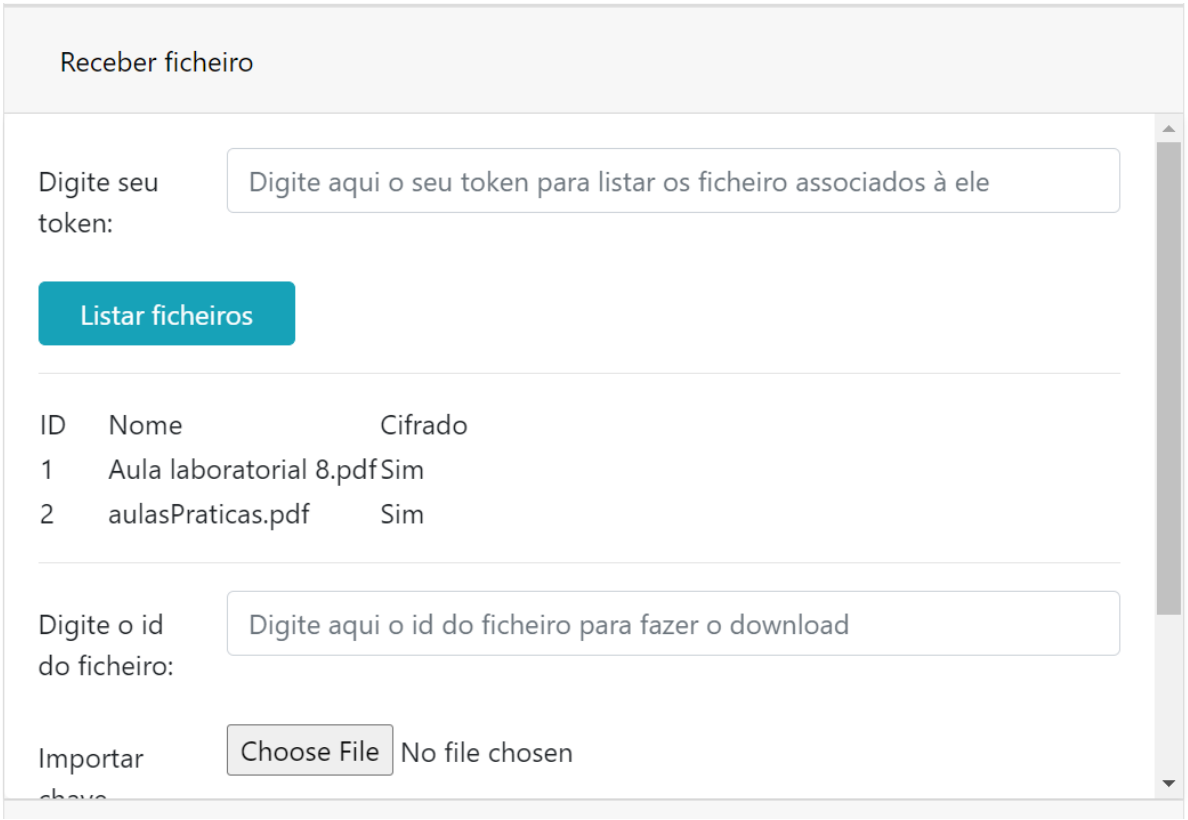
D. Quando terminar, clique no botão "Enviar" (Submeter).". Assim, o ficheiro será enviado para o token selecionado com as configurações desejadas.

Receber ficheiros



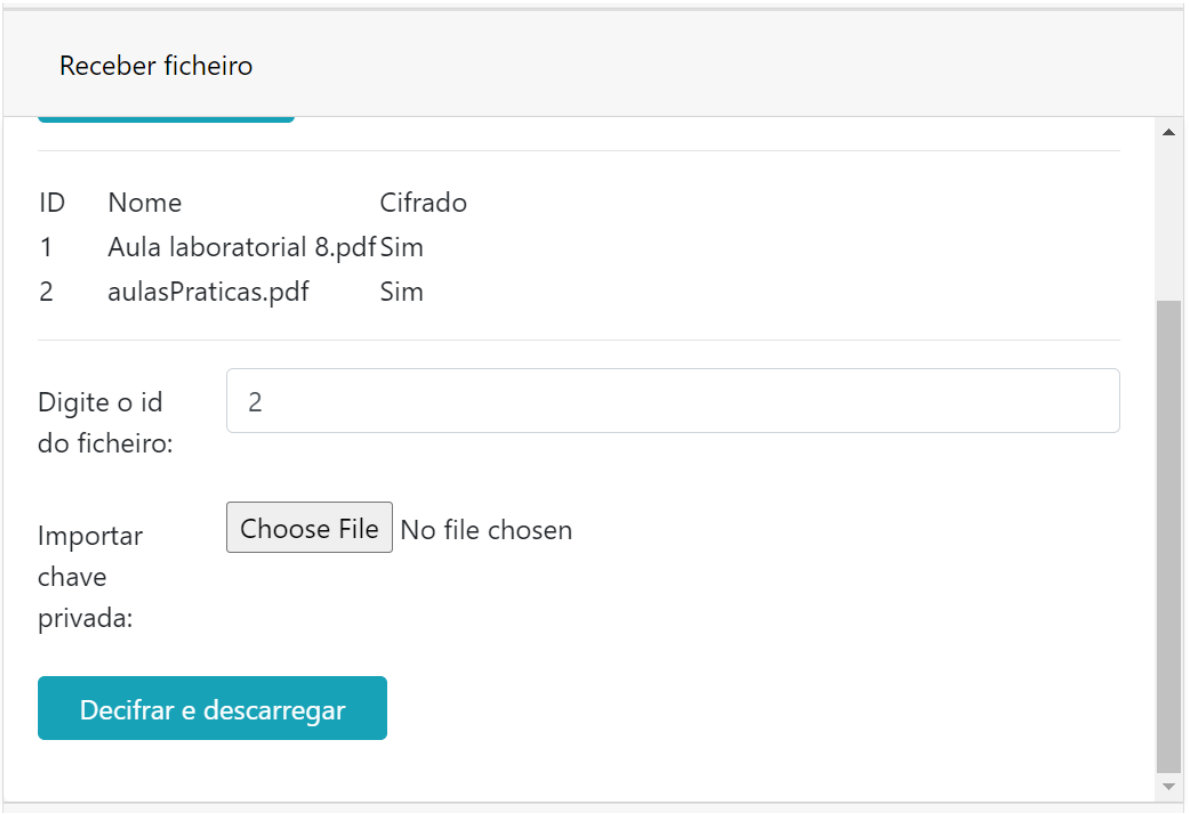
A. Listar Ficheiros:

Esta é a secção superior, que lhe permite introduzir o seu token para ver todos os ficheiros que lhe foram enviados. Depois de clicar no botão "Listar ficheiros", terá de abrir novamente esta secção e será apresentada uma tabela com as informações como na imagem seguinte:

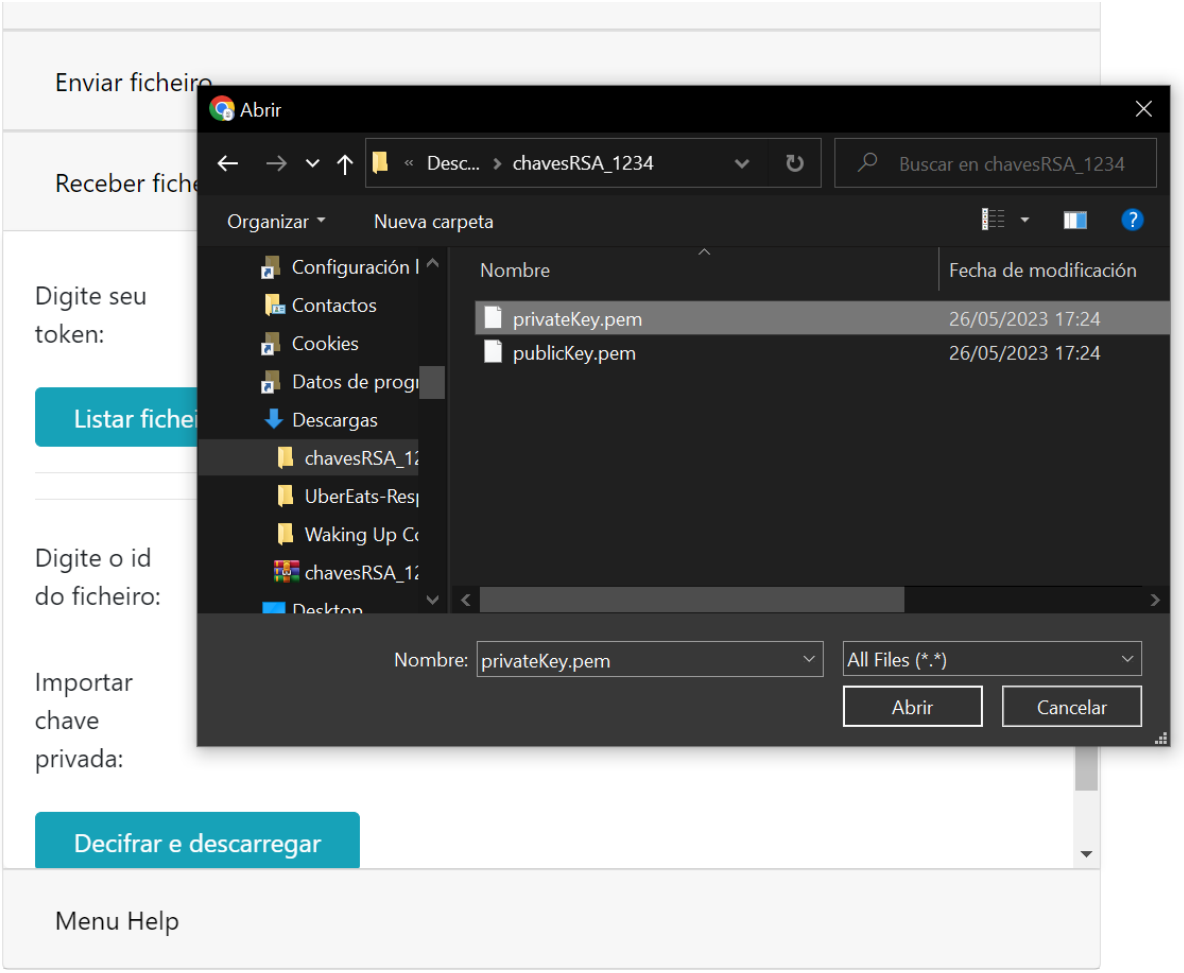


Mostrando o ID que é o identificador do aquivo no sistema, o nome original e se está cifrado ou não. Deste passo, o mais importante é o ID que utilizaremos para poder descarregar o arquivo.

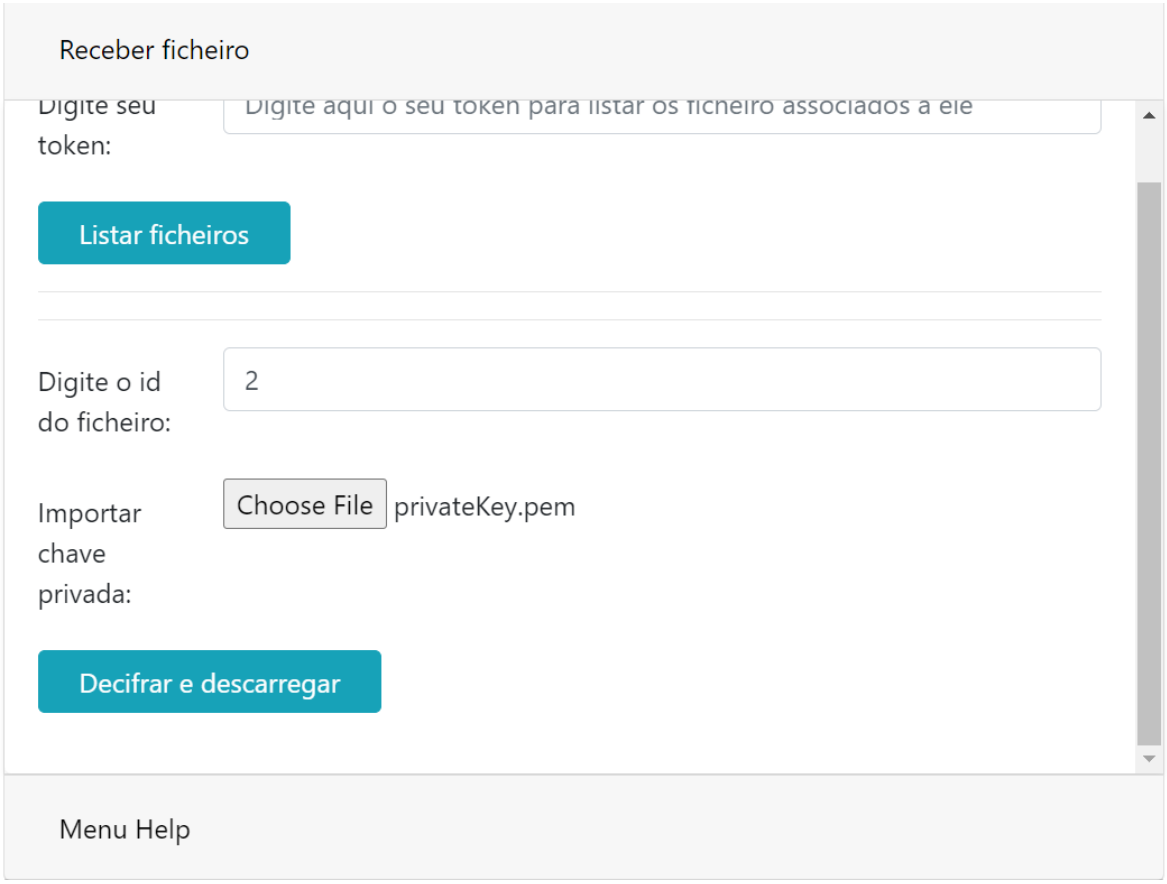
B. Descarregar Ficheiro:



Só temos de escrever o ID do ficheiro que queremos descarregar e, no caso de estar encriptado, na parte "Importar chave privada:", utilizando o botão "Choose File" (Escolher ficheiro), abre-se uma janela como a da imagem seguinte:



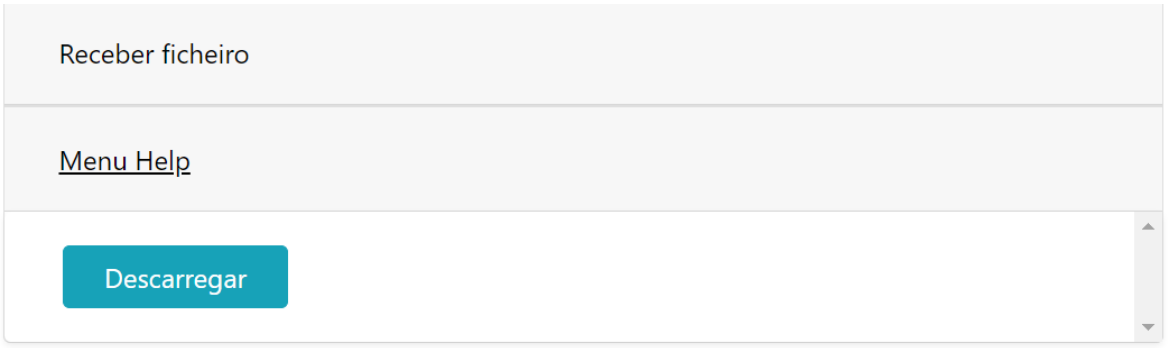
Procuramos nos directórios a chave privada que foi gerada pela aplicação e selecionamos o ficheiro “privateKey.pem” com a respectiva chave privada válida.



Depois só temos de clicar no botão "Decifrar e descarregar". E teremos o ficheiro descarregado e decifrado no nosso computador.

Se o ficheiro não estiver encriptado, pode descarregá-lo sem utilizar a chave privada.

Menu Help:



Esta é a secção onde, clicando no botão "Descarregar", pode descarregar este manual em formato pdf.

Preguntas Frequentes:

A. Como é que a informação é processada e como é protegida?

A geração das chaves é criada no lado do cliente, pelo que as suas chaves não chegam ao servidor, apenas a chave pública é transmitida posteriormente para que outros utilizadores possam encriptar os ficheiros por si.

Não armazenamos informações como o correio electrónico, nem as chaves privadas, pelo que, se perder a sua chave privada, não há recuperação. Também não temos um sistema de login de utilizador para aumentar o anonimato e a segurança.

B. O que devo fazer se perder a minha chave privada?

Não poderá descarregar os ficheiros enviados para o seu token, mas não entre em pânico, ninguém poderá descarregá-los, a menos que tenham sido roubados... nesse caso, é melhor notificar todas as pessoas que lhe enviam ficheiros.

Pode criar um novo token e esquecer que alguma vez teve um…

C. O que devo fazer se me esquecer do meu token?

Se se esquecer do seu token, não poderá listar os ficheiros que lhe foram enviados. Pode criar um novo token e pedir que os ficheiros sejam reenviados para o seu novo token. A sua segurança é importante para nós e não armazenamos os seus dados.

D. Como é que sei que ninguém, para além do remetente, irá ler os ficheiros?

Enquanto os ficheiros estiverem encriptados, apenas a pessoa que tiver a chave privada do token para o qual os enviou poderá descarregar o ficheiro e desencriptá-lo.

E. Posso apresentar conteúdos restringidos por legislação governamental?

Oferecemos apenas um serviço de armazenamento e um meio de comunicação, a utilização do serviço e as suas consequências são da responsabilidade dos utilizadores.

F. Existe alguma possibilidade de os meus conteúdos encriptados serem desencriptados por terceiros?

Actualmente, é impossível fazê-lo em tempo real, mas com o advento de novas tecnologias, como a computação quântica, no futuro deixaremos de ter essa certeza.

Lembre-se sempre que só deve ser possível utilizando a chave privada, por isso cuide bem dela.