

**Como compilar o projeto**

**Compilar as classes relativas ao servidor:**

javac -d bin src/Server/SeiTchizServer.java src/Server/CatalogoClientes.java src/Server/CatalogoGrupos.java src/Server/Cliente.java src/Server/Grupo.java src/Server/Mensagem.java src/Server/Photo.java src/Server/Autenticacao.java

**Compilar a classe relativa ao cliente:**

javac -d bin src/Client/SeiTchiz.java

**Como executar o projeto com os ficheiros de permissões**

**Exemplo de comandos para execução do servidor:**

**Executar ficheiro .class:**

java -cp bin -Djava.security.manager -Djava.security.policy==server.policy Server.SeiTchizServer 45678 servidor servidor

**Executar ficheiro .jar:**

java -cp bin -Djava.security.manager -Djava.security.policy==server.policy -jar SeiTchizServer.jar 45678 servidor servidor

**Exemplo de comandos para execução do cliente:**

**Executar o ficheiro .class:**

java -cp bin -Djava.security.manager -Djava.security.policy==client.policy Client.SeiTchiz 127.0.0.1:45678 truststore\_client clientid clientid clientid

java -cp bin -Djava.security.manager -Djava.security.policy==client.policy Client.SeiTchiz 127.0.0.1:45678 truststore\_client manelteste manelteste manelteste

java -cp bin -Djava.security.manager -Djava.security.policy==client.policy Client.SeiTchiz 127.0.0.1:45678 truststore\_client mantorras mantorras Mantorras

**Executar ficheiro .jar:**

java -cp bin -Djava.security.manager -Djava.security.policy==client.policy -jar SeiTchiz.jar 127.0.0.1:45678 truststore\_client clientid clientid clientid

java -cp bin -Djava.security.manager -Djava.security.policy==client.policy -jar SeiTchiz.jar 127.0.0.1:45678 truststore\_client manelteste manelteste manelteste

java -cp bin -Djava.security.manager -Djava.security.policy==client.policy -jar SeiTchiz.jar 127.0.0.1:45678 truststore\_client mantorras mantorras mantorras

**Passwords das keystores dos utilizadores correspondentes**

**Username - Password**

clientid – clientid

maneltest – maneltest

mantorras – mantorras

**Truststore Client - Password**

truststore\_client - servidor

**Decisões de desenho das soluções implementadas**

Para organização do trabalho relativamente a cliente-servidor separámos o código de modo a ter os ficheiros relacionados ao servidor dentro da pasta ./data/ e os ficheiros locais do cliente em pastas na ./root/.

Dentro do ./data/ temos 3 pastas que contêm o que o próprio nome indica. Primeiro, na pasta relativamente a ficheiros de grupo temos subpastas para cada grupo individual em que cada um tem os ficheiros de: histórico de mensagens, caixa de mensagens, e membros de cada grupo. As keys dos grupos que servirão para cifrar e decifrar as mensagens (que será feito do lado do cliente) encontram-se fora do domínio do servidor, na root, em ./GroupKeys/, cuja pasta tem um ficheiro por grupo com os membros e chaves associadas para cada momento em que houve mudança de chave. Como os ficheiros relativos ao servidor têm de ser protegidos, ciframos os mesmos para termos apenas ficheiros com a extensão .cif que não podem ser lidos por intrusos. No entanto, para realizarmos a cifra, usamos um ficheiro auxiliar .txt para escrever a informação que queremos que depois irá ser cifrado num .cif e eliminado.

//encriptar para fich aux

TODO

FALAR DO PATH DAS KEYSTORES, TRUST…..

As keystores dos clientes

**Limitações do trabalho**

As fotografias usadas para o comando Post devem estar dentro da pasta "test" na raiz do projeto (devido a permissoes dos policies).

A mensagem enviada para os grupos nao deve conter "%%" (é uma palavra reservada para tratamento de ficheiros).

A pasta bin não pode ser apagada, apenas devem ser apagados os seus conteúdos.

O nome do utilizador ou do grupo nao devem conter ":" (é um caracter reservado para tratamento de ficheiros).