



universidade de aveiro

Departamento de Eletrónica, Telecomunicações e Informática

Segurança

IEDCS: Identity Enabled Distribution Control System

Suplemento ao relatório – Casos de Uso

Curso [8240] MI em Engenharia de Computadores e Telemática
Disciplina [47232] Segurança
Ano Letivo 2015/2016

Alunos [64090] Rui Lebre
[68129] Tomás Rodrigues
Prática P1
Docente Professor João Paulo Barraca

Aveiro, 30 de Dezembro de 2015

Introdução

Serve o presente documento para demonstrar um dos vários casos de uso do sistema IEDCS desenvolvido para a componente prática da unidade curricular de Segurança. Daqui em diante, irá ser utilizado o termo ‘servidor’ como referência ao servidor IEDCS, responsável por autenticar utilizadores e distribuir conteúdos, ‘cliente’ referente ao reprodutor de conteúdos transferidos pelo nosso IEDCS, e ‘utilizador’ referente a qualquer utilizador do *player* e que requiere conteúdos do servidor.

O sistema admite que toda e qualquer cópia está devidamente registada no servidor, através de uma chave única usada para o efeito – *player key* – e que aquando o requisito de nova ligação, essa chave é verificada e assim dada ou não permissão ao *player* para continuar a ligação. No caso da *player key* não constar na base de dados, a ligação já estabelecida é encerrada abruptamente pelo servidor, impedido assim a execução de mais ações à partida.

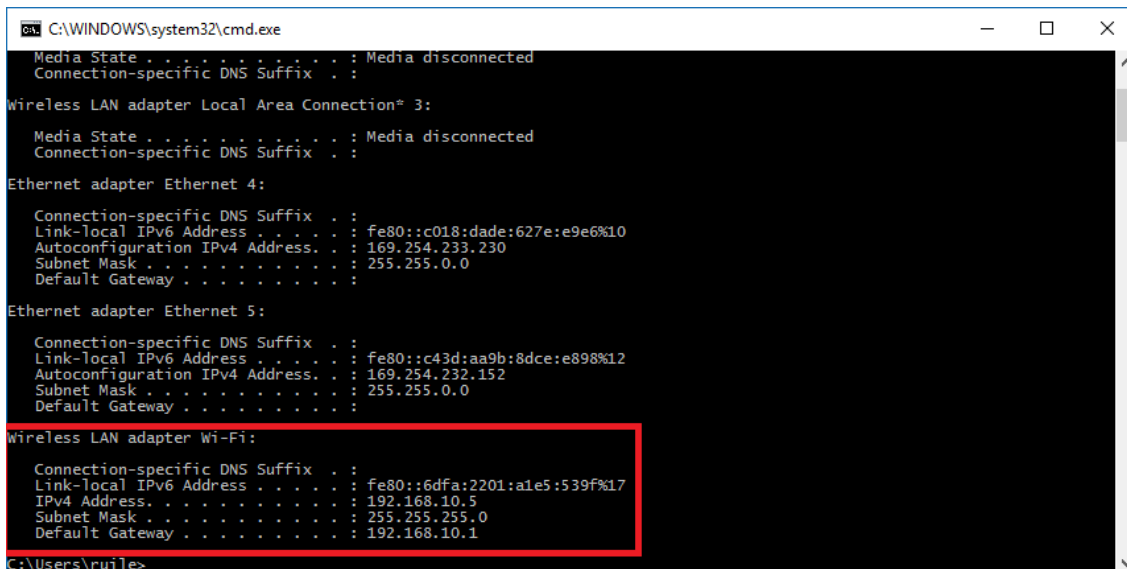
Na demonstração que se segue, o servidor irá ser executado numa máquina virtual com Xubuntu 14.04.2 de 32 bits, em modo bridged com a placa de rede wi-fi. Por sua vez, o servidor de base de dados MySQL irá estar a ser executado no host, assim como o player.

A demonstração será feita com especial enfoque ao utilizador. Porém, ao longo deste suplemento, ir-se-á mostrar também estados do servidor, bem como a sua instalação e execução.

Casos de Uso

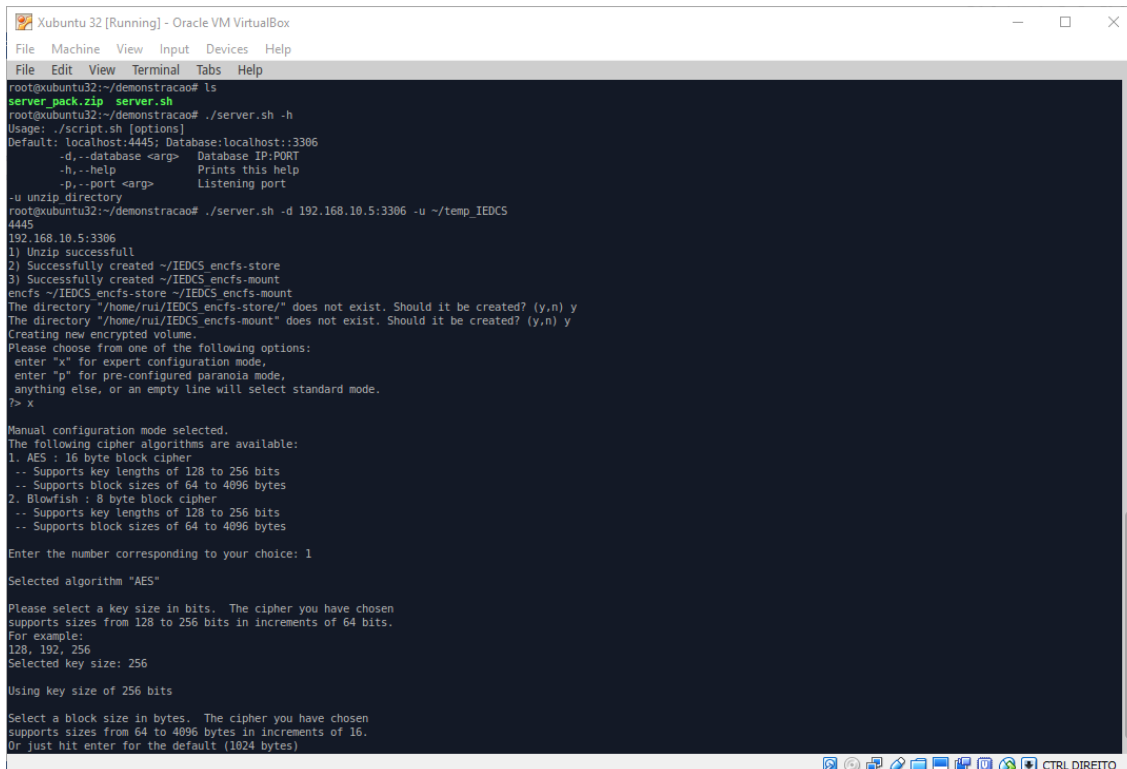
1. Instalação e execução do servidor

a) Execução do *Shell script* server.sh e configuração do sistema de ficheiros (ecnfs)



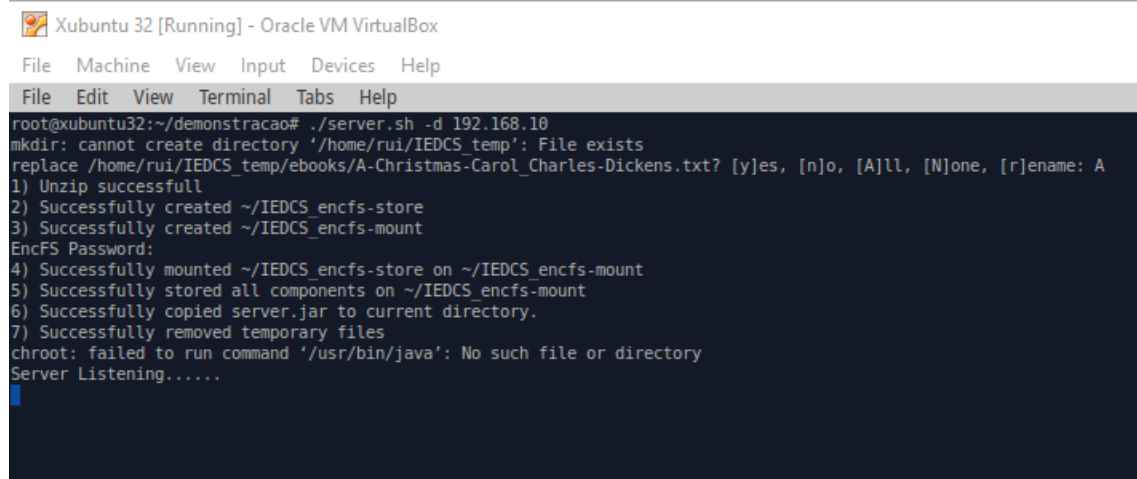
```
C:\WINDOWS\system32\cmd.exe
Media State . . . . . : Media disconnected
Connection-specific DNS Suffix  : 
Wireless LAN adapter Local Area Connection* 3:
Media State . . . . . : Media disconnected
Connection-specific DNS Suffix  : 
Ethernet adapter Ethernet 4:
Connection-specific DNS Suffix  : 
Link-local IPv6 Address . . . . : fe80::c018:dade:627e:e9e6%10
Autoconfiguration IPv4 Address. . : 169.254.233.230
Subnet Mask . . . . . : 255.255.0.0
Default Gateway . . . . . : 
Ethernet adapter Ethernet 5:
Connection-specific DNS Suffix  : 
Link-local IPv6 Address . . . . : fe80::c43d:aa9b:8dce:e898%12
Autoconfiguration IPv4 Address. . : 169.254.232.152
Subnet Mask . . . . . : 255.255.0.0
Default Gateway . . . . . : 
Wireless LAN adapter Wi-Fi:
Connection-specific DNS Suffix  : 
Link-local IPv6 Address . . . . : fe80::6dfa:2201:a1e5:539f%17
IPv4 Address. . . . . : 192.168.10.5
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 192.168.10.1
C:\Users\ruile>
```

Figura 1 - Verificação do IP do host que contém a base de dados



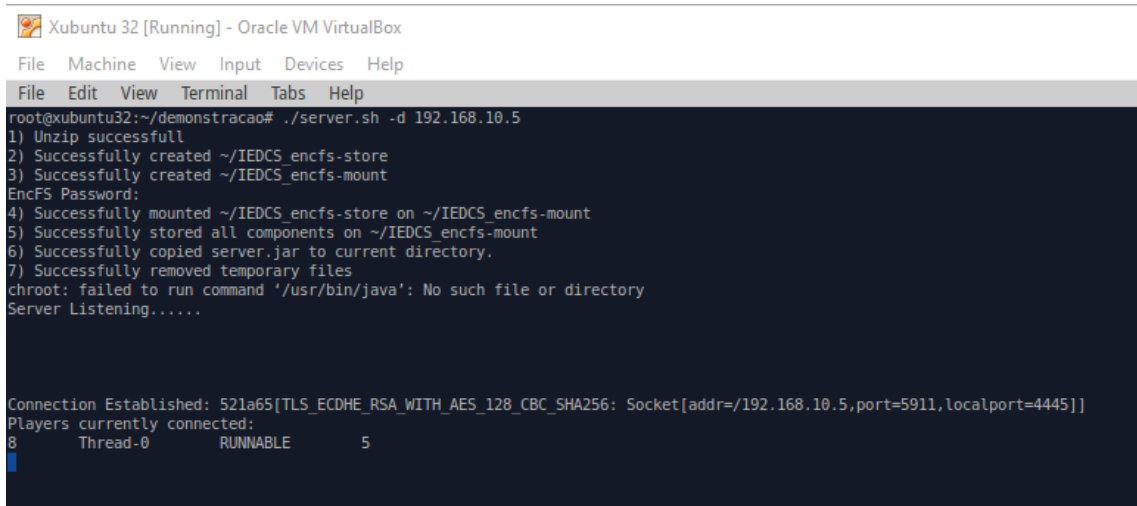
```
Xubuntu 32 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
File Edit View Terminal Tabs Help
root@xubuntu32:~/demonstracao# ls
server_pack.zip server.sh
root@xubuntu32:~/demonstracao# ./server.sh -h
Usage: ./script.sh [options]
Default: localhost:4445; Database:localhost::3306
-d,--database <arg> Database IP:PORT
-h,--help Prints this help
-p,--port <arg> Listening port
-u unzip_directory
root@xubuntu32:~/demonstracao# ./server.sh -d 192.168.10.5:3306 -u ~/temp_IEDCS
4445
192.168.10.5:3306
1) Unzip successfull
2) Successfully created ~/IEDCS_encfs-store
3) Successfully created ~/IEDCS_encfs-mount
encfs ~/IEDCS_encfs-store ~/IEDCS_encfs-mount
The directory "/home/ruil/IEDCS_encfs-store/" does not exist. Should it be created? (y,n) y
The directory "/home/ruil/IEDCS_encfs-mount" does not exist. Should it be created? (y,n) y
Creating new encrypted volume.
Please choose from one of the following options:
enter "x" for expert configuration mode,
enter "p" for pre-configured paranoia mode,
anything else, or an empty line will select standard mode.
?> x
Manual configuration mode selected.
The following cipher algorithms are available:
1. AES : 16 byte block cipher
-- Supports key lengths of 128 to 256 bits
-- Supports block sizes of 64 to 4096 bytes
2. Blowfish : 8 byte block cipher
-- Supports key lengths of 128 to 256 bits
-- Supports block sizes of 64 to 4096 bytes
Enter the number corresponding to your choice: 1
Selected algorithm "AES"
Please select a key size in bits. The cipher you have chosen
supports sizes from 128 to 256 bits in increments of 64 bits.
For example:
128, 192, 256
Selected key size: 256
Using key size of 256 bits
Select a block size in bytes. The cipher you have chosen
supports sizes from 64 to 4096 bytes in increments of 16.
Or just hit enter for the default (1024 bytes)
```

Figura 2 – Execução do Script



```
Xubuntu 32 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
File Edit View Terminal Tabs Help
root@xubuntu32:~/demonstracao# ./server.sh -d 192.168.10
mkdir: cannot create directory '/home/rui/IEDCS temp': File exists
replace /home/rui/IEDCS_temp/ebooks/A-Christmas-Carol_Charles-Dickens.txt? [y]es, [n]o, [A]ll, [N]one, [r]ename: A
1) Unzip successfull
2) Successfully created ~/IEDCS_encfs-store
3) Successfully created ~/IEDCS_encfs-mount
EncFS Password:
4) Successfully mounted ~/IEDCS_encfs-store on ~/IEDCS_encfs-mount
5) Successfully stored all components on ~/IEDCS_encfs-mount
6) Successfully copied server.jar to current directory.
7) Successfully removed temporary files
chroot: failed to run command '/usr/bin/java': No such file or directory
Server Listening.....
```

Figura 3 – Execução do Script e servidor pronto a receber novos pedidos



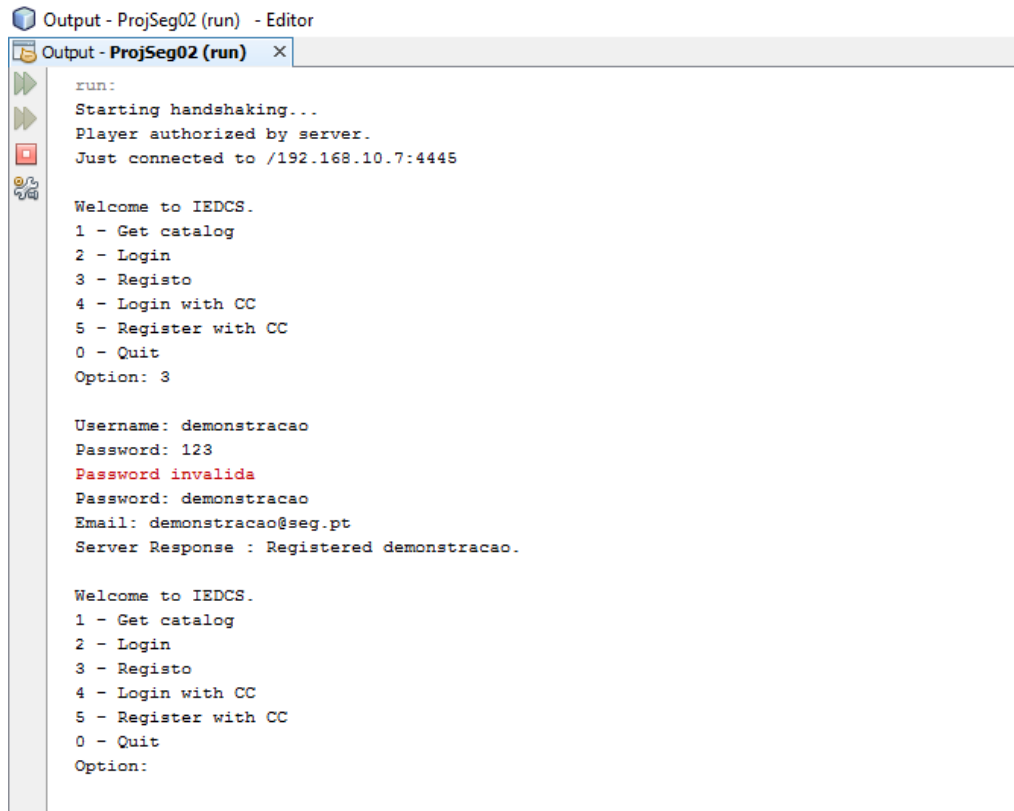
```
Xubuntu 32 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
File Edit View Terminal Tabs Help
root@xubuntu32:~/demonstracao# ./server.sh -d 192.168.10.5
1) Unzip successfull
2) Successfully created ~/IEDCS_encfs-store
3) Successfully created ~/IEDCS_encfs-mount
EncFS Password:
4) Successfully mounted ~/IEDCS_encfs-store on ~/IEDCS_encfs-mount
5) Successfully stored all components on ~/IEDCS_encfs-mount
6) Successfully copied server.jar to current directory.
7) Successfully removed temporary files
chroot: failed to run command '/usr/bin/java': No such file or directory
Server Listening.....

Connection Established: 521a65[TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256: Socket[addr=/192.168.10.5,port=5911,localport=4445]]
Players currently connected:
8      Thread-0      RUNNABLE      5
```

Figura 4 – Receção de um pedido de estabelecimento de ligação e sua consumação

2. Registo e login utilizando credenciais

- a) Registo utilizando o utilizador 'demonstracao' com a password '123'
- b) Registo utilizando o utilizador 'demonstracao' com a password 'demonstracao'
- c) Login utilizando o utilizador 'demonstracao'
- d) Listagem dos títulos disponíveis
- e) Compra de um título
- f) Requisição do título
- g) Mudança da *password*



```
run:
Starting handshaking...
Player authorized by server.
Just connected to /192.168.10.7:4445

Welcome to IEDCS.
1 - Get catalog
2 - Login
3 - Registo
4 - Login with CC
5 - Register with CC
0 - Quit
Option: 3

Username: demonstracao
Password: 123
Password invalida
Password: demonstracao
Email: demonstracao@seg.pt
Server Response : Registered demonstracao.

Welcome to IEDCS.
1 - Get catalog
2 - Login
3 - Registo
4 - Login with CC
5 - Register with CC
0 - Quit
Option:
```

Figura 5 – Demonstração das alíneas a) Registo utilizando o utilizador 'demonstracao' com a password '123' e b) Registo utilizando o utilizador 'demonstracao' com a password 'demonstracao'

```

Welcome to IEDCS.
1 - Get catalog
2 - Login
3 - Registo
4 - Login with CC
5 - Register with CC
0 - Quit
Option: 2

Username: demonstracao
Password: demonstracao
Server Response : Logged in as demonstracao.

Login as demonstracao
1 - Get catalog
2 - Search on catalog
3 - Purchase item
4 - Retrieve item
5 - Settings
6 - Logout
0 - Exit application
Option: |

```

Figura 6 – Demonstração da alínea c) Login utilizando o utilizador 'demonstracao'

```

Server Listening.....

Connection Established: 521a65[TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256: Socket[addr=/192.168.10.5,port=5911,localport=4445]]
Players currently connected:
8      Thread-0      RUNNABLE      5

Connection Established: 5e5487[TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256: Socket[addr=/192.168.10.5,port=5937,localport=4445]]
Players currently connected:
8      Thread-0      RUNNABLE      5
11     Thread-2      RUNNABLE      5

Users currently connected:
11     Thread-2      demonstracao

```

Figura 7 – Estado do servidor após fecho de uma comunicação, abertura de uma nova e login do utilizador 'demonstracao'

```

Login as demonstracao
1 - Get catalog
2 - Search on catalog
3 - Purchase item
4 - Retrieve item
5 - Settings
6 - Logout
0 - Exit application
Option: 1

```

ID	Titulo	Autor	Data Pub.
1	Titulo de Teste	Autor de Teste	14/11/2015
2	A Christmas Carol	Charles Dickens	14/11/2015
3	A Tale of Two Cities	Charles Dickens	14/11/2015
4	Agulha em Palheiro	Camilo Castelo Branco	14/11/2015
5	Alices Adventures in Wonderland	Lewis Carroll	14/11/2015
6	Amor de Perdicao	Camilo Castelo Branco	14/11/2015
7	Amor de Salvacao	Camilo Castelo Branco	14/11/2015
8	Annos de Prosa	Camilo Castelo Branco	14/11/2015
9	Beowulf	Lesslie Hall	14/11/2015
10	Carlota Angela	Camilo Castelo Branco	14/11/2015
11	Contos dAldeia	Alberto Braga	14/11/2015
12	Contos para a infancia	Guerra Junqueiro	14/11/2015
13	Desperate Choices	Jeanette Cooper	14/11/2015
14	Estrellas Funestas	Camilo Castelo Branco	14/11/2015
15	Estrellas Propicias	Camilo Castelo Branco	14/11/2015
16	Frankenstein or The Modern Prometheus	Mary Wollstonecraft	14/11/2015
17	Great Expectations	Charles Dickens	14/11/2015
18	Moby Dick	Herman Melville	14/11/2015
19	Pride and Prejudice	Jane Austen	14/11/2015
20	Redemption s Warrior	Jennifer Morse and William Mortimer	14/11/2015
21	The Adventures of Sherlock Holmes	Arthur Conan Doyle	14/11/2015
22	The Adventures of Tom Sawyer	Mark Twain	14/11/2015
23	The Diaries of Bunty Danvers	Patricia Ainger	14/11/2015
24	The Identity Check	Ken Merrell	14/11/2015
25	The Importance of Being Earnest	Oscar Wilde	14/11/2015
26	The Picture of Dorian Gray	Oscar Wilde	14/11/2015
27	The Yellow Wallpaper	Charlotte Perkins Gilman	14/11/2015
28	Ulysses	James Joyce	14/11/2015

Figura 8 – Demonstração da alínea d) Listagem dos títulos disponíveis

ID	Titulo	Autor	Data Pub.
1	Titulo de Teste	Autor de Teste	14/11/2015
2	A Christmas Carol	Charles Dickens	14/11/2015
3	A Tale of Two Cities	Charles Dickens	14/11/2015

Login as demonstracao
 1 - Get catalog
 2 - Search on catalog
 3 - Purchase item
 4 - Retrieve item
 5 - Settings
 6 - Logout
 0 - Exit application
 Option: 3
 Item ID (0 - Cancel): 2
 Server Response : Sucessfully purchased.

Figura 9 – Demonstração da alínea e) Compra de um título

1 - Get catalog
 2 - Search on catalog
 3 - Purchase item
 4 - Retrieve item
 5 - Settings
 6 - Logout
 0 - Exit application
 Option: 4

ID	Titulo	Autor	Data Pub.
1	Titulo de Teste	Autor de Teste	14/11/2015
2	A Christmas Carol	Charles Dickens	14/11/2015

Item ID (0 - Cancel): 2

Enter to continue reading. To cancel streaming, type 'cancel' or '0'.

The Project Gutenberg EBook of A Christmas Carol, by Charles Dickens

This eBook is for the use of anyone anywhere at no cost and with almost no restrictions whatsoever. You may copy it, give it away or re-use it under the terms of the Project Gutenberg License included with this eBook or online at www.gutenberg.net

Title: A Christmas Carol
 A Ghost Story of Christmas

Author: Charles Dickens

Release Date: August 11, 2004 [EBook #46]

Language: English

*** START OF THIS PROJECT GUTENBERG EBOOK A CHRISTMAS CAROL ***

Figura 10 – Demonstração da alínea f) Requisição do título


```
Login as demonstracao
1 - Get catalog
2 - Search on catalog
3 - Purchase item
4 - Retrieve item
5 - Settings
6 - Logout
0 - Exit application
Option: 5
```

```
Login as demonstracao
1 - Change e-mail
2 - Change password
3 - Show bought items
4 - Back
0 - Exit application
Option: 2
Actual password: demonstracao
New password: segurancas2015
Server Response : Password successfully changed.
```

```
Welcome to IEDCS.
1 - Get catalog
2 - Login
3 - Registo
4 - Login with CC
5 - Register with CC
0 - Quit
Option: 2

Username: demonstracao
Password: demonstracao
Server Response : Error - connection refused.
```

```
Welcome to IEDCS.
1 - Get catalog
2 - Login
3 - Registo
4 - Login with CC
5 - Register with CC
0 - Quit
Option: 2

Username: demonstracao
Password: segurancas2015
Server Response : Logged in as demonstracao.
```

Figuras 11 e 12 – Demonstração da alínea g) Mudança da password

3. Registo e Login utilizando o Cartão do Cidadão

- a) Registo utilizando o utilizador 'demonstracaocc'
- b) Login utilizando cartão do cidadão
- c) Requisição do título

```
run:
Starting handshaking...
Player authorized by server.
Just connected to localhost/127.0.0.1:4445
```

```
Welcome to IEDCS.
1 - Get catalog
2 - Login
3 - Registo
4 - Login with CC
5 - Register with CC
0 - Quit
Option: 5

Username: demonstracaocc
Email: demonstracaocc@seg.pt
Insert smartcard and password
```

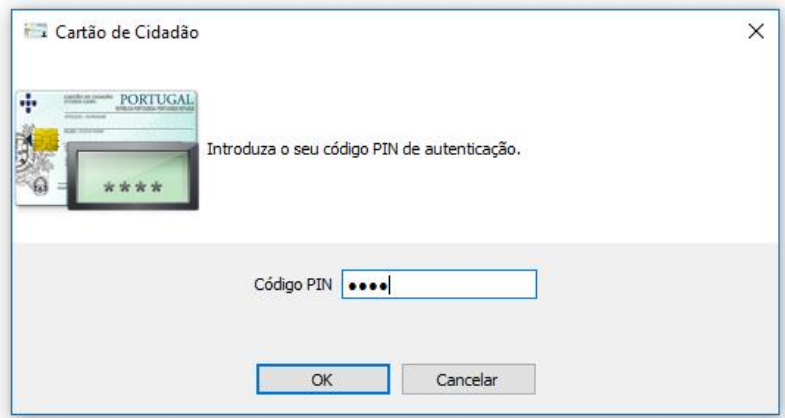


Figura 13 – Demonstração da alínea a) Registo utilizando o utilizador 'demonstracaocc'

```
Welcome to IEDCS.
1 - Get catalog
2 - Login
3 - Registo
4 - Login with CC
5 - Register with CC
0 - Quit
Option: 4
Server Response : Logged in as RUI LEBRE.
```

```
Login as RUI LEBRE
1 - Get catalog
2 - Search on catalog
3 - Purchase item
4 - Retrieve item
5 - Settings
6 - Logout
0 - Exit application
Option:
```

Figura 14 – Demonstração da alínea b) Login utilizando cartão do cidadão

```

Login as RUI LEBRE
1 - Get catalog
2 - Search on catalog
3 - Purchase item
4 - Retrieve item
5 - Settings
6 - Logout
0 - Exit application
Option: 3
Item ID (0 - Cancel): 17
Server Response : Sucessfully purchased.

```

```

Login as RUI LEBRE
1 - Get catalog
2 - Search on catalog
3 - Purchase item
4 - Retrieve item
5 - Settings
6 - Logout
0 - Exit application
Option: 4

```

ID	Titulo	Autor	Data Pub.	
1	Titulo de Teste	Autor de Teste	14/11/2015	
2	A Christmas Carol	Charles Dickens	14/11/2015	
17	Great Expectations	Charles Dickens	14/11/2015	

```

Item ID (0 - Cancel): 17

```

```

Enter to continue reading. To cancel streaming, type 'cancel' or '0'.

```

```

-----
The Project Gutenberg EBook of Great Expectations, by Charles Dickens

```

```

This eBook is for the use of anyone anywhere at no cost and with
almost no restrictions whatsoever. You may copy it, give it away or
re-use it under the terms of the Project Gutenberg License included

```

Figura 15 – Demonstração da alínea c) Requisição do título

that Philip Pirrip, late of this parish, and also Georgiana wife of the above, were dead and buried; and that Alexander, Bartholomew, Abraham, Tobias, and Roger, infant children of the aforesaid, were also dead and buried; and that the dark flat wilderness beyond the churchyard, intersected with dikes and mounds and gates, with scattered cattle feeding on it, was the marshes; and that the low leaden line beyond was the river; and that the distant savage lair from which the wind was rushing was the sea; and that the small bundle of shivers growing afraid of it all and beginning to cry, was Pip.

"Hold your noise!" cried a terrible voice, as a man started up from among the graves at the side of the church porch. "Keep still, you little devil, or I'll cut your throat!"

A fearful man, all in coarse gray, with a great iron on his leg. A man with no hat, and with broken shoes, and with an old rag tied round his head. A man who had been soaked in water, and smothered in mud, and lamed by stones, and cut by flints, and stung by nettles, and torn by briars; who limped, and shivered, and glared, and growled; and whose teeth chattered in his head as he seized me by the chin.

"Oh! Don't cut my throat, sir," I pleaded in terror. "Pray don't do it, sir."

"Tell us your name!" said the man. "Quick!"

"Pip, sir."

"Once more," said the man, staring at me. "Give it mouth!"

"Pip. Pip, sir."

"Show us where you live," said the man. "Pint out the place!"

I pointed to where our village lay, on the flat in-shore among the alder-trees and pollards, a mile or more from the church.

3

Enter to continue reading. To cancel streaming, type 'cancel' or '0'.

Figura 16 – Continuação da leitura do e-book após requisição de páginas

Caso de uso do servidor

```
Connection Established: 9b55a00[TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256: Socket(addr=/127.0.0.1,port=6433,localport=4445)]
Players currently connected:
12 Thread-0 TERMINATED 5
15 Thread-2 TERMINATED 5
17 Thread-3 RUNNABLE 5
19 Thread-4 TERMINATED 5
22 Thread-5 RUNNABLE 5
25 Thread-6 RUNNABLE 5
30 Thread-7 RUNNABLE 5
Sucessfully purchased.
Header: 0B89D1706A92061C66E38A3271B30096, File: F15B6CBC9F6F6122677726902DA5D7D3, Device: B73D1FC752354718F21959FDE6739CF9, Player: 085548D000DDE7487B99F40DC15D6075
ebooks\\Great-Expectations_Charles-Dickens.txt
```

Neste caso pode-se observar vários *players* ligados ao servidor e outros já terminados. Pretende-se enaltecer que, quando foi feito um pedido, a resposta a este é acompanhada com um Header (explicação detalhada no relatório) deduzido a partir das chaves na imagem “Player”, “Device” e “File”.

Para a decifragem do ebook, é necessário deduzir File key através do Header. O servidor tem um papel importante neste passo, uma vez que sem a sua compactuação é impossível ao player decifrar o ebook.