**Secure Web Application**

**SWA**

**Team Members**

Ahmad Abuashour(6144926)

Prosenjit Sinha(9190740)

Akram Bouktab()

Rebbeca Gideon(9329935)

Revision History

|  |  |  |  |
| --- | --- | --- | --- |
| **Date** | **Version** | **Description** | **Author** |
| <01/Nov/08> | <1.0> | Initial version | Team |
| <05/Nov/08> | <1.1> | Intermediate version | Team |
| <20/Nov/08> | <1.2> | Intermediate version | Team |
| <01/Dec/08> | <1.3> | Final version | Team |

Table of Contents

1. Introduction 4

1.1 Purpose 4

1.2 Scope 4

1.3 Definitions, Acronyms, and Abbreviations 4

1.4 References 5

1.5 Overview 6

2. Use-Case View 7

2.1 Actors 7

2.2 Use-Cases 8

3. Logical View 9

3.1 Overview 9

3.2 Architecturally Significant Design Packages 9

3.3 Significant Sequence Diagrams 10

3.4 Data Base Model 12

4. Interface Description 14

4.1 Browser configuration 14

4.2 User interfaces 15

4.2.1 Home page 15

4.2.2 Documents list page 15

4.2.3 Users list page 16

4.2.4 Create a new user 16

4.2.5 Capability list page 17

4.2.6 Access Control list page 17

4.2.7 Logs list page 18

5. Components deployment and configuration 19

5.1 Network configuration 19

5.2 Certificates management 20

5.3 Servers configuration 21

5.3.1 Web Server configuration 21

5.3.2 PHP configuration 23

5.3.3 DataBase server configuration 24

5.3.4 LDAP Server configuration 26

5.3.5 SSL/TLS validation 28

6. Size and Performance 30

7. Quality 30

# Introduction

## Purpose

The purpose of this document is to describe the design that we made to realise the Secure Web Application. Secure Web Application allow user to store his files using a Web pages and allow administrator to manage users that can accede to this application.

The Secure Web Application uses PKI infrastructure to authenticate users. When user tries to connect, he gives his certificate. Then the web server, in collaboration with the LDAP server, checks the validity of this certificate. The LDAP server is a server Directory that will store all users’ certificates.

When the user is authenticated, he can do operations depending on his privilege (Administrator or simple user). All communications between principals of the Secure Web Application are made over SSL.

## Scope

The Secure Web Application supports two different users:

* A simple user that can upload, download, delete and view files that he can access too.
* An administrator that have user’s right and also right add, delete users and to manage their capability list.

The principal goal of this secure application is to a specific data base by preventing any illegal person to access to this data base and see its content.

## Definitions, Acronyms, and Abbreviations

The following table provides a list of terms that are used in this document and a brief explanation for each term.

|  |  |
| --- | --- |
| ***Term*** | ***Definition*** |
| *SWA* | *Software Secure Application, the name of our application project.* |
| *Apache* | *Open source HTTP server.* |
| *OpenSSL* | *Open source implementation of the SSL and TLS protocols.* |
| *OpenLDAP* | *Open source implementation of the Lightweight Directory Access Protocol.* |
| *MySQL* | *Open source relational database management system* |
| *CA* | *Certification authority.* |
| *ACL* | *Access control list.* |
| *C\_List* | *Capability list.* |
| *DER* | *Distinguished Encoding Rules* |
| *PEM* | *Privacy Enhanced Mail* |
| *HTTP* | *Hypertext Transfer Protocol* |
| *PKCS* | *Public Key Cryptographic* |
| *SSL/TLS* | *Secure Sockets Layer/Transport layer security* |
| *PHP* | *Hypertext Preprocessor* |

## References

|  |  |
| --- | --- |
| *RFC2251* | *Lightweight Directory Access Protocol version 3* |
| *RFC2616* | *Hypertext Transfer Protocol version 1.1* |
| *RFC2818* | *HTTP over TLS (https)* |
| *RFC4346* | *Transport Layer Security(TLS) protocol version 1.1* |
| [*http://httpd.apache.org/docs*](http://httpd.apache.org/docs) | *Apache web server documentation* |
| [*http://www.php.net/docs.php*](http://www.php.net/docs.php) | *PHP documentation* |
| [*http://dev.mysql.com/doc*](http://dev.mysql.com/doc) | *MySQL documentation* |
| [*http://ww.openldap.org/doc*](http://ww.openldap.org/doc) | *OpenLDAP documentation* |
| *IEEE Std 1016-1998* | *Recommended Practice for SDD* |
| [*http://www.upedu.org/upedu/*](http://www.upedu.org/upedu/) | *Software Process* |

## Overview

This SWA aims to build a secure web application that allows user to request services in secure way. In this system, we are using encryption technique to encrypt all sessions between principals.

The SWA is composed of three main principles, First: openLDAP is a service directory that contains client information and responsible to store the user certificate, second: web server that is considered as a central principal and its responsibility is to authenticate the user and serve him web pages depending on his privilege. Finally: Data base server is the principle who stores all users’ documents.

The rest of this document describes the environment that will affect the product and its requirement; it also goes in more details for requirement.

# Use-Case View



Figure : Use Case Diagram

## Actors

|  |  |
| --- | --- |
| *User* | *User can view files list, delete existing file, upload a new file and download existing files.* |
| *Administrator* | *Administrator inherits from user meaning that he can do whatever the user can do. Also, he can delete existing user, add a new user, modify the ACL of existing file, modify the capability list of existing user, generate certificate for new user.* |

## Use-Cases

|  |  |
| --- | --- |
| *Manage files* | |
| *View* | *Depending on his privilege, the user can view a list of available files in the data base.* |
| *Delete* | *Depending on his privilege, the user can delete existing file.* |
| *Download* | *Depending on his privilege, the user can download existing file.* |
| *Upload* | *User can upload new file.* |

|  |  |
| --- | --- |
| *Manage users* | |
| *Add* | *Administrator can add a new user.* |
| *Delete* | *Administrator can delete existing user.* |
| *ACL* | *Administrator can modify access control list for each file.* |
| *C\_List* | *Administrator can modify control list for each user.* |
| *Generate Certificate* | *Administrator can generate new certificate.* |

# Logical View

## Overview

This section describes significant parts of the design model, such as packages, sequence diagrams, database model.

## Architecturally Significant Design Packages



Figure : Package diagram

|  |  |
| --- | --- |
| *Web* | *This package contains all software components that are responsible to generate web pages to serve the client.* |
| *CA* | *This package contains all software components that are responsible to create certificate.* |
| *LDAP* | *This package contains all software components that allow web component to communicate with LDAP server.* |
| *SQL* | *This package contains all software components that allow web component to communicate with SQL server.* |

## Significant Sequence Diagrams



Figure : Connection Sequence diagram



Figure : ‘Download document’ Sequence diagram

## Data Base Model

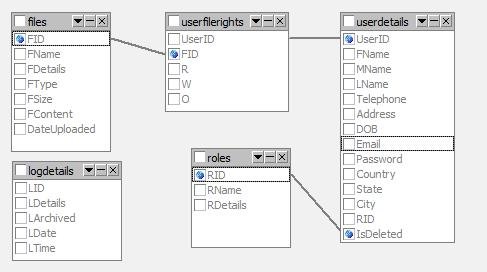


Figure : Database Structure

|  |  |
| --- | --- |
| *Files* | |
| *FID* | *String: Unique file Id used as primary key.* |
| *FName* | *String: File name.* |
| *FDetails* | *String: Description associated to this file when uploaded.* |
| *FType* | *String: File type, (exe, doc, img…)* |
| *FSize* | *Integer: File size.* |
| *FContent* | *MEDIUMBLOB: File data content.* |
| *DateUploaded* | *Date: Datewhen his file was uploaded to database.* |

|  |  |
| --- | --- |
| *UserFileRights* | |
| *UserID* | *String: Id user, foreign key, reference to the UserDetails table.* |
| *FID* | *String: Id file, foreign key, reference to the Files table.* |
| *R* | *Boolean: representing Read right.* |
| *W* | *Boolean: representing Write right.* |
| *O* | *Boolean: representing Own right.* |

|  |  |
| --- | --- |
| *Roles* | |
| *RID* | *String: Unique role Id used as primary key.* |
| *RName* | *String: Role name.* |
| *RDetails* | *String: Role description.* |

|  |  |
| --- | --- |
| *LogDetails* | |
| *LID* | *String: Unique log Id used as primary key.* |
| *LDetails* | *String: Log details information.* |
| *LArchived* | *Boolean: Archive the current log.* |
| *LDate* | *Date: date of the current log.* |
| *LTime* | *Date: time of the current log.* |

|  |  |
| --- | --- |
| *UserDetails* | |
| *IserID* | *String: Unique user Id used as primary key.* |
| *FName* | *String: user first name.* |
| *MName* | *String: user middle name.* |
| *LName* | *String: user last name.* |
| *Telephone* | *String: user phone.* |
| *Address* | *String: user address.* |
| *Email* | *String: user email address.* |
| *Country* | *String: user country.* |
| *State* | *String: user state.* |
| *City* | *String: user city.* |

# Interface Description

## Browser configuration

Since we are dealing with a web application, the client is supposed to use a web browser to show web pages. We are using Internet Explorer Browser. Following screen shot to import pkcs12 key store inside IE to allow mutual authentication with Web Server:

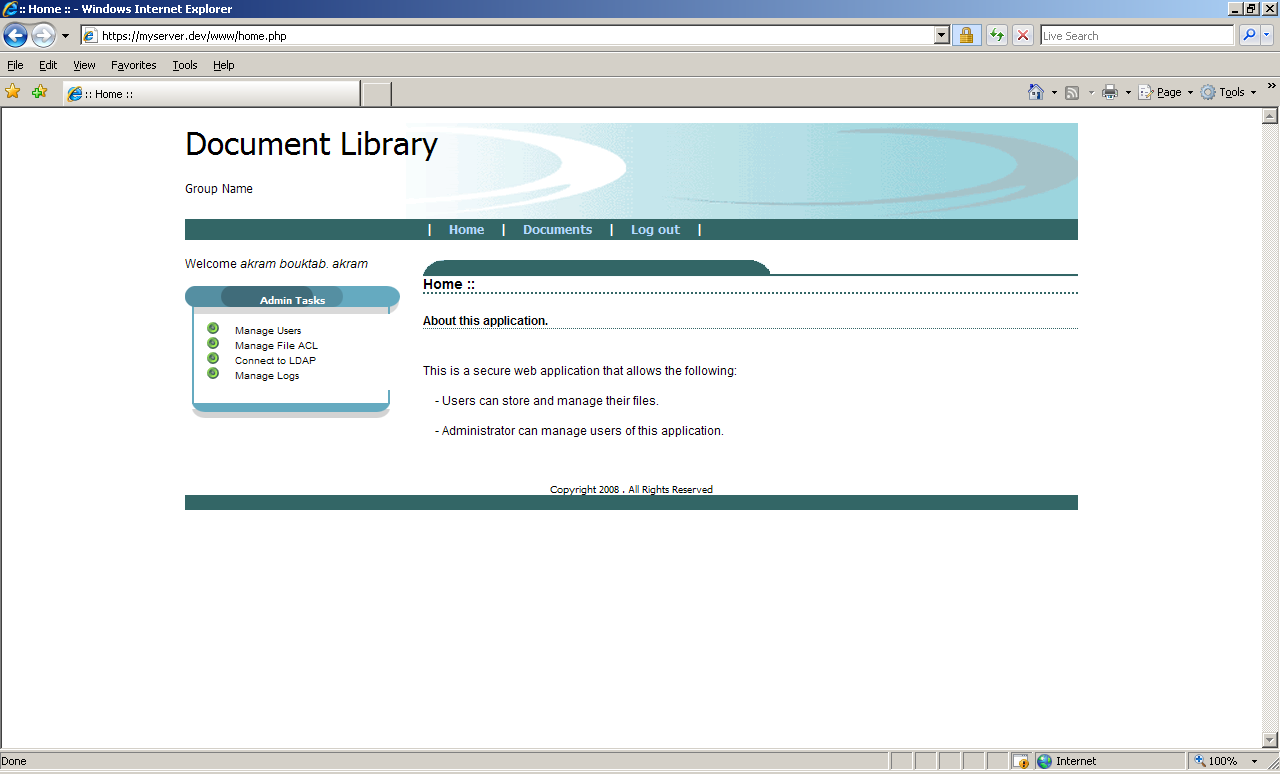
|  |
| --- |
|  |

|  |
| --- |
|  |

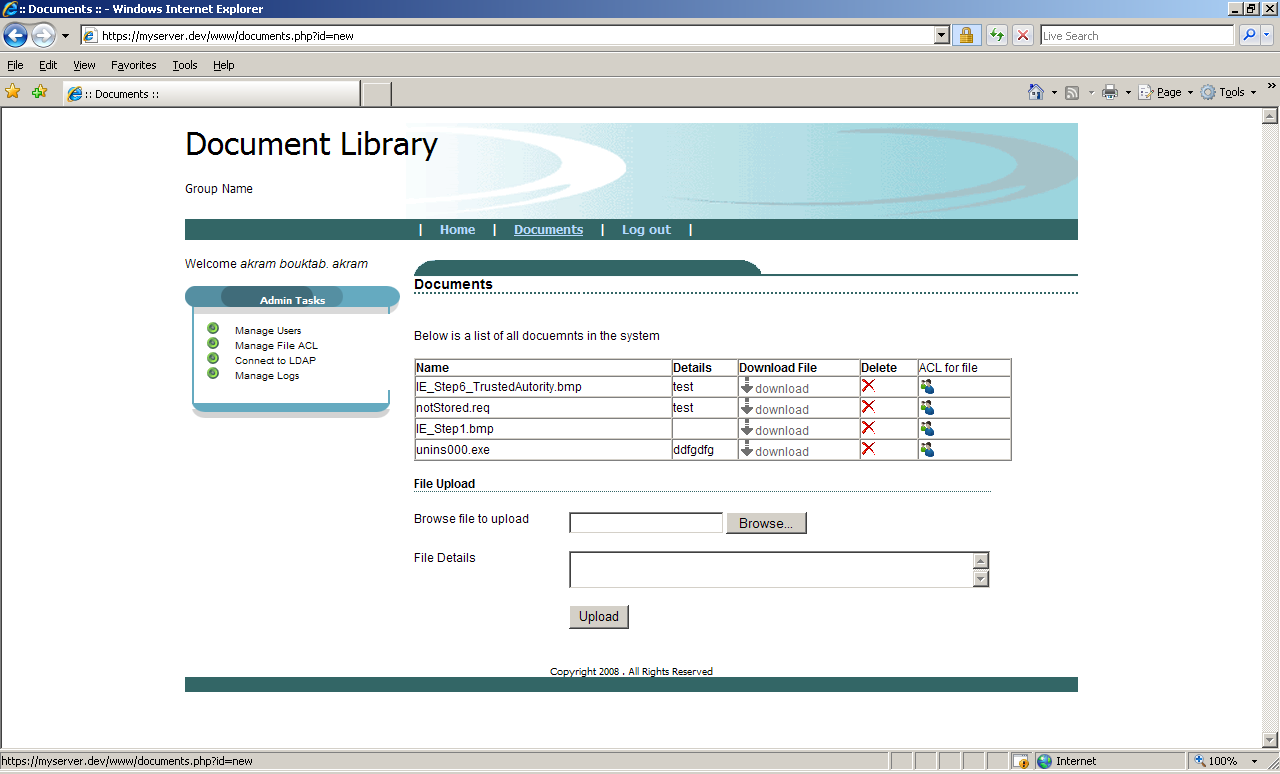
|  |
| --- |
|  |

## User interfaces

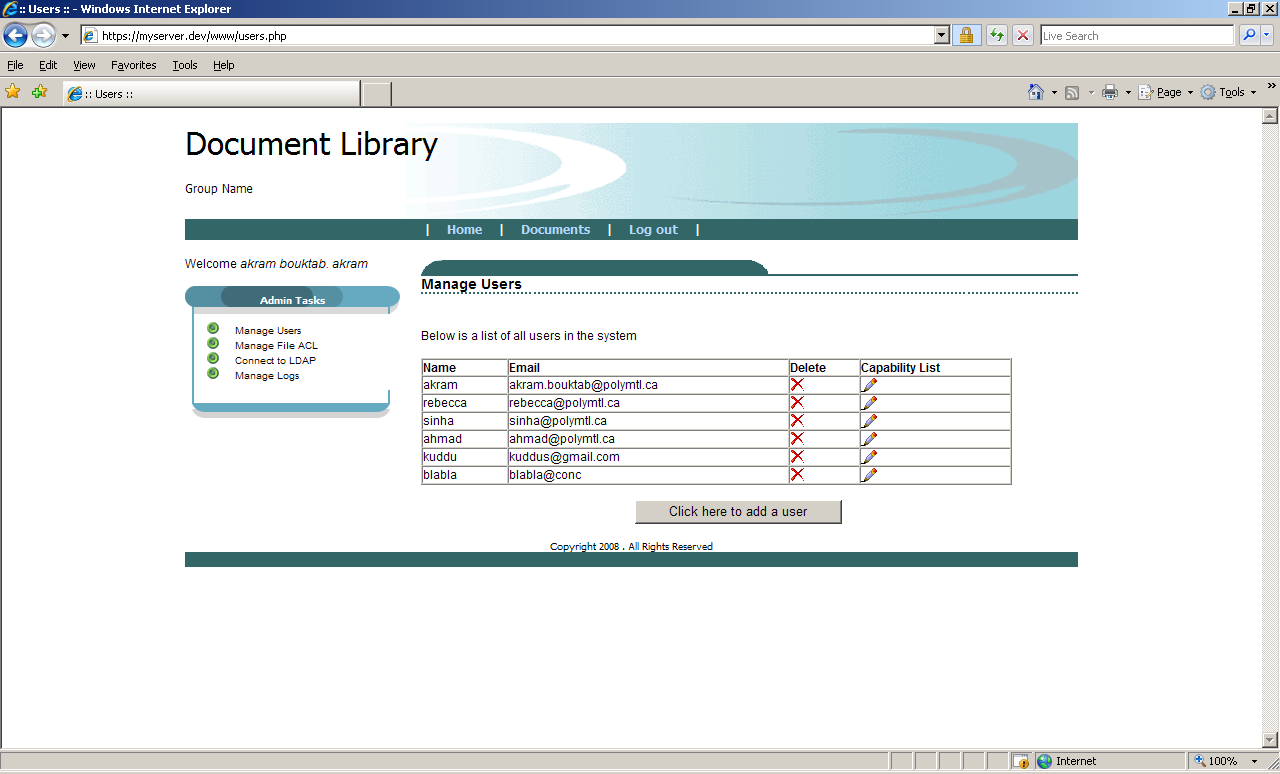
### Home page

****

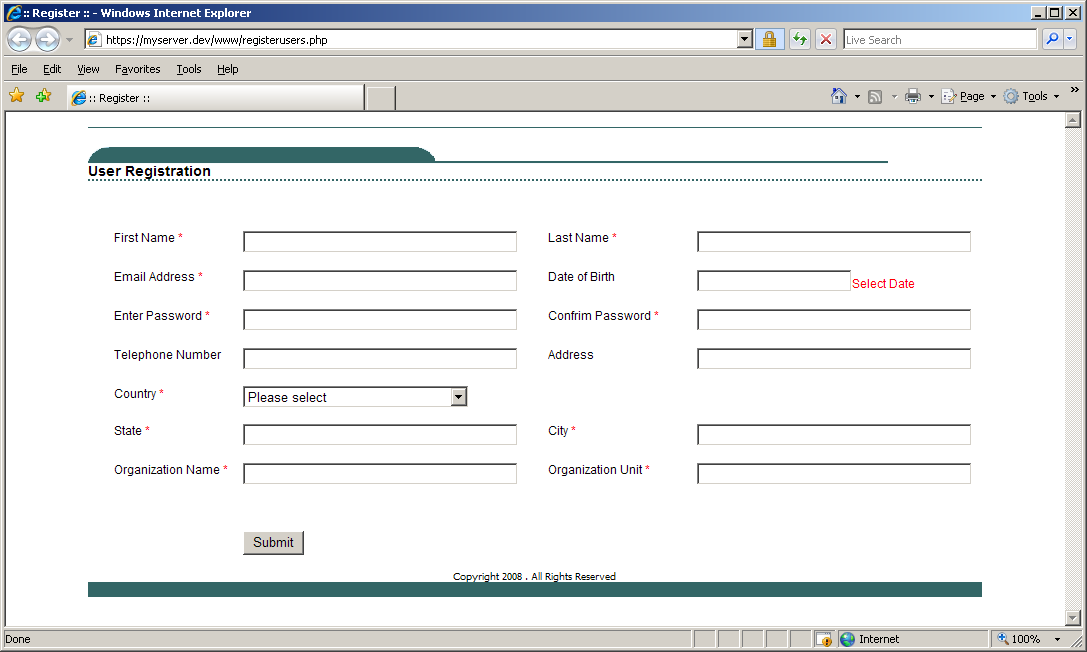
### Documents list page

****

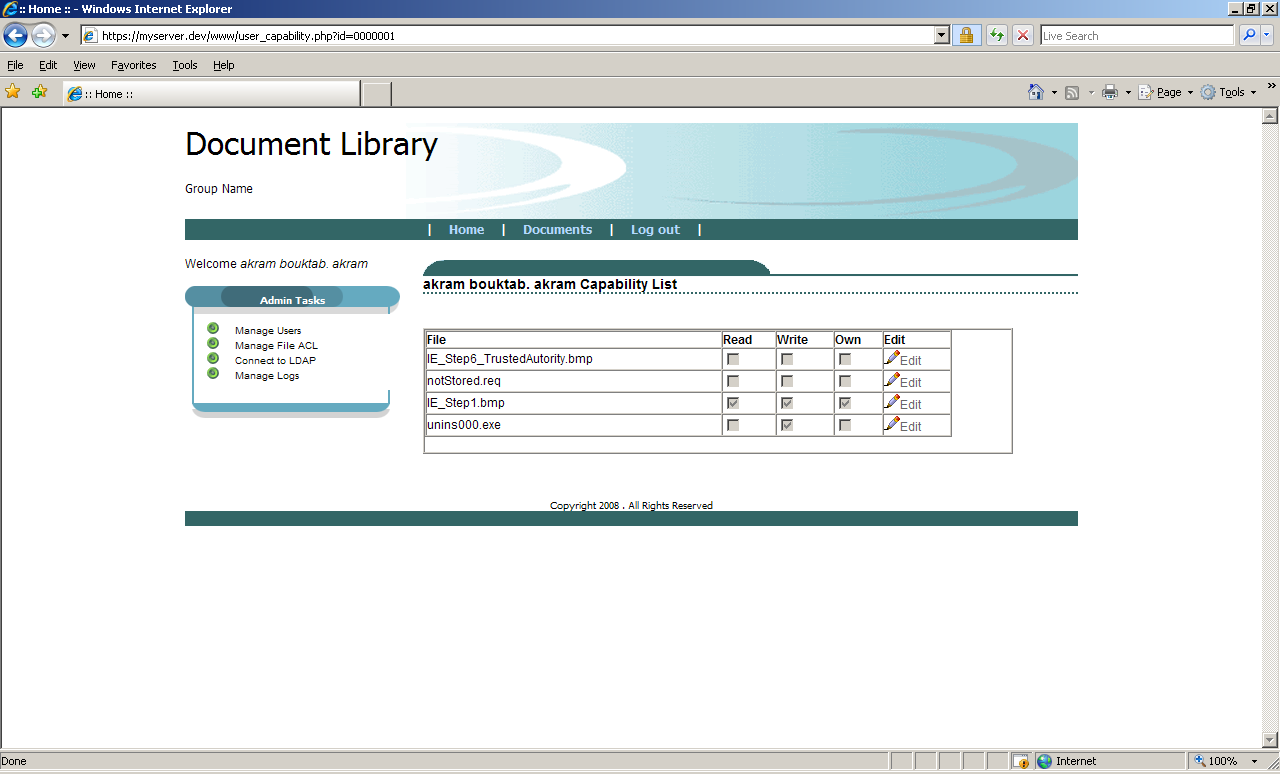
### Users list page

****

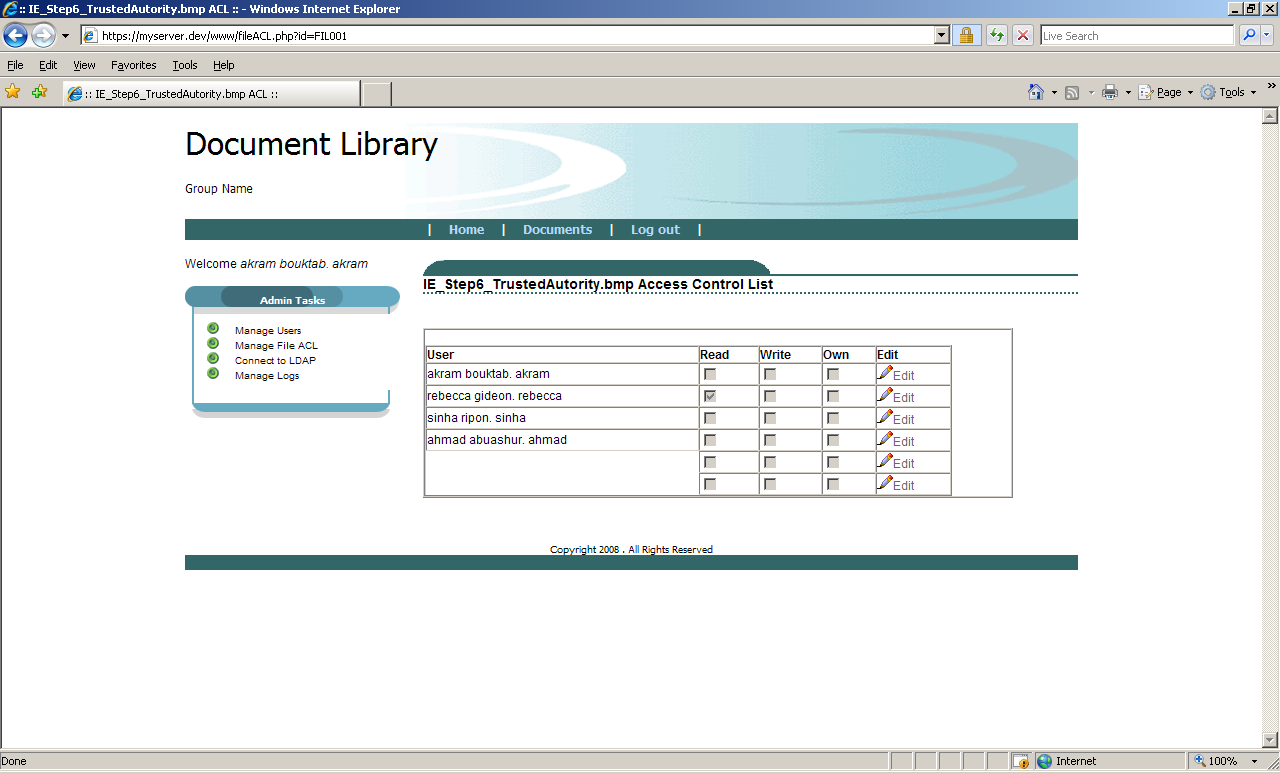
### Create a new user



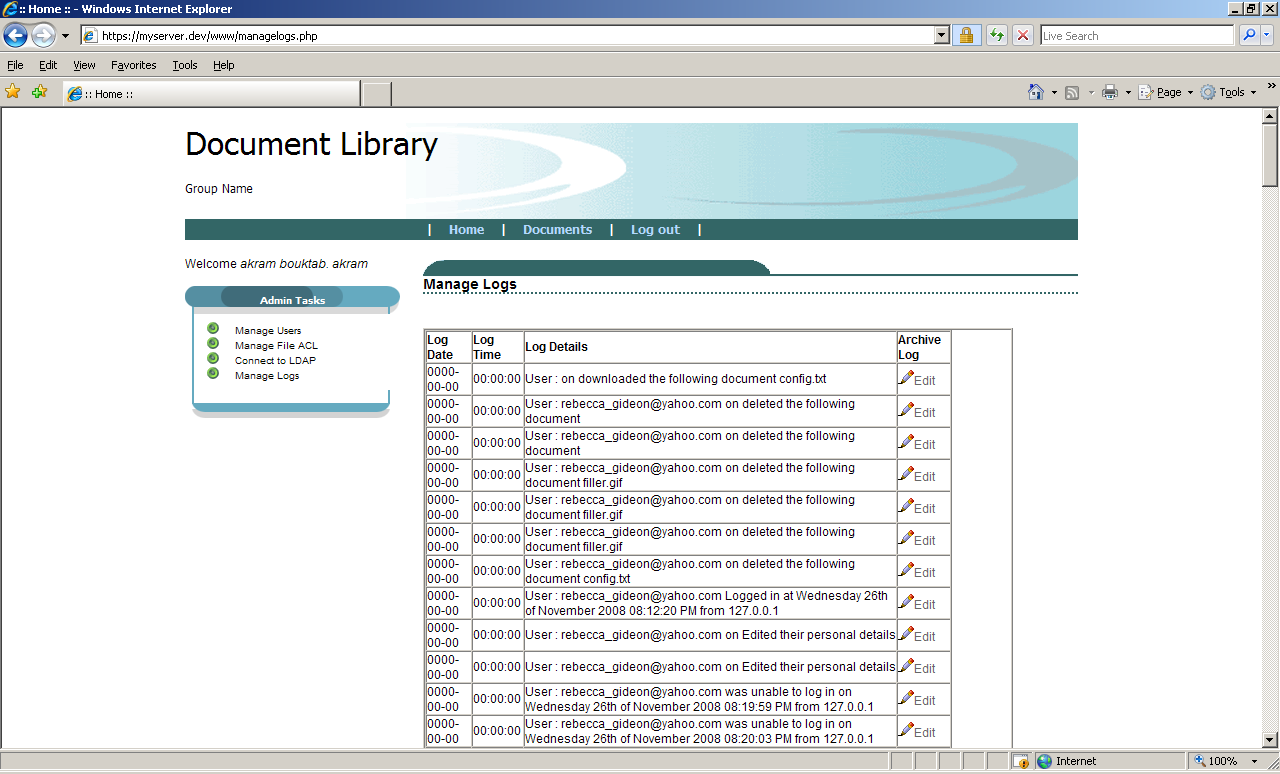
### Capability list page

****

### Access Control list page

****

### Logs list page

****

# Components deployment and configuration

## Network configuration

|  |
| --- |
|  |

Following the client requirement, we need in our project three servers machine and one user machine for test. All those machines are built in virtual machines inside the same computer as following:

* Each principal in this project is represented by its own virtual machine with its own configuration.
* Since there is no DHCP server in our emulated network, we are using static IP address for each machine.
* Since there is no DNS server in our network, we aredefining static resolution in every machine “C:\WINDOWS\system32\drivers\etc\hosts” to build resolution.

|  |
| --- |
| C:\WINDOWS\system32\drivers\etc\hosts  127.0.0.1 localhost  169.254.48.100 User  169.254.48.101 myserver  169.254.48.101 myserver.dev  169.254.48.101 www.myserver.dev  169.254.48.101 ApacheServer  169.254.48.102 MySQLServer  169.254.48.103 OpenLDAPServer |

## Certificates management

|  |
| --- |
|  |

In this configuration, every principal have to trust the CA and must have CA certificate. When a principal generate his own pair (private key, public key), he send to CA to be signed. When principal are communicating, they can validate their certificates each other because those certificates are signed by the same trusted authority.

The CA uses OpenSSL to generate certificates and use the following script to generate a private key, a certificate, a pkcs12 key store and a der certificate format:

|  |
| --- |
| CA\_GenerateKey.bat: parameter = ca,  Executed one time to generate CA certificate.  openssl genrsa 2048 > ca.key  openssl req -new -x509 -nodes -days 1000 -key ca.key > ca.cer  openssl pkcs12 -export -in ca.cer -inkey ca.key -out ca.p12 |
| principal\_GenerateKey.bat: parameter = principal  Executed for every principal and every user.  openssl req -newkey rsa:2048 -days 1000 -nodes -keyout %1.key > %1.req  openssl x509 -req -in %1.req -days 1000 -CA ca.cer -CAkey ca.key -set\_serial 01 > %1.cer  openssl pkcs12 -export -in %1.cer -inkey %1.key -out %1.p12  openssl x509 -outform DER -in %1.cer -out %1.der |

## Servers configuration

### Web Server configuration

The web server used for this project is Apache. Following the ‘httpd.conf’ file that contains all configuration of web server for this deployment:

|  |
| --- |
| ServerRoot "C:/Program Files/Apache Software Foundation/Apache2.2"  Listen 80  Listen 443  LoadModule actions\_module modules/mod\_actions.so  LoadModule alias\_module modules/mod\_alias.so  LoadModule asis\_module modules/mod\_asis.so  LoadModule auth\_basic\_module modules/mod\_auth\_basic.so  LoadModule authn\_default\_module modules/mod\_authn\_default.so  LoadModule authn\_file\_module modules/mod\_authn\_file.so  LoadModule authz\_default\_module modules/mod\_authz\_default.so  LoadModule authz\_groupfile\_module modules/mod\_authz\_groupfile.so  LoadModule authz\_host\_module modules/mod\_authz\_host.so  LoadModule authz\_user\_module modules/mod\_authz\_user.so  LoadModule autoindex\_module modules/mod\_autoindex.so  LoadModule cgi\_module modules/mod\_cgi.so  LoadModule dir\_module modules/mod\_dir.so  LoadModule env\_module modules/mod\_env.so  LoadModule include\_module modules/mod\_include.so  LoadModule isapi\_module modules/mod\_isapi.so  LoadModule log\_config\_module modules/mod\_log\_config.so  LoadModule mime\_module modules/mod\_mime.so  LoadModule negotiation\_module modules/mod\_negotiation.so  LoadModule rewrite\_module modules/mod\_rewrite.so  LoadModule php5\_module "C:/Program Files/Apache Software Foundation/php/php5apache2\_2.dll"  PHPIniDir "C:/Program Files/Apache Software Foundation/php"  LoadModule setenvif\_module modules/mod\_setenvif.so  LoadModule ssl\_module modules/mod\_ssl.so  <IfModule !mpm\_netware\_module>  <IfModule !mpm\_winnt\_module>  User daemon  Group daemon  </IfModule>  </IfModule>  ServerAdmin akram.bouktab@polymtl.ca  ServerName localhost:80  DocumentRoot "C:/Program Files/Apache Software Foundation/www/myserver.dev/public\_html"  <Directory />  Options FollowSymLinks  AllowOverride None  Order deny,allow  Deny from all  </Directory>  <Directory "C:/Program Files/Apache Software Foundation/www/myserver.dev/public\_html">  Options Indexes FollowSymLinks  AllowOverride None  Order allow,deny  Allow from all  </Directory>  <IfModule dir\_module>  DirectoryIndex index.html index.php  </IfModule>  <FilesMatch "^\.ht">  Order allow,deny  Deny from all  Satisfy All  </FilesMatch>  ErrorLog "logs/error.log"  LogLevel warn  <IfModule log\_config\_module>  LogFormat "%h %l %u %t \"%r\" %>s %b \"%{Referer}i\" \"%{User-Agent}i\"" combined  LogFormat "%h %l %u %t \"%r\" %>s %b" common  <IfModule logio\_module>  LogFormat "%h %l %u %t \"%r\" %>s %b \"%{Referer}i\" \"%{User-Agent}i\" %I %O" combinedio  </IfModule>  CustomLog "logs/access.log" common  </IfModule>  <IfModule alias\_module>  ScriptAlias /cgi-bin/ "C:/Program Files/Apache Software Foundation/Apache2.2/cgi-bin/"  </IfModule>  <IfModule cgid\_module>  </IfModule>  <Directory "C:/Program Files/Apache Software Foundation/Apache2.2/cgi-bin">  AllowOverride None  Options None  Order allow,deny  Allow from all  </Directory>  DefaultType text/plain  <IfModule mime\_module>  TypesConfig conf/mime.types  AddType application/x-compress .Z  AddType application/x-gzip .gz .tgz  AddType application/x-httpd-php .php  AddType application/x-httpd-php-source .phps  </IfModule>  Include conf/extra/httpd-vhosts.conf  <IfModule ssl\_module>  SSLRandomSeed startup builtin  SSLRandomSeed connect builtin  </IfModule>  SSLMutex default  SSLRandomSeed startup builtin  SSLSessionCache none  <VirtualHost localhost:443>  SSLEngine On  SSLCertificateFile "C:/OpenSSL/keyStore/ApacheServer.cer"  SSLCertificateKeyFile "C:/OpenSSL/keyStore/ApacheServer.key"  SSLCACertificateFile "C:/OpenSSL/keyStore/ca.cer"  SSLVerifyClient require  SSLOptions +StdEnvVars +StrictRequire +ExportCertData  SSLVerifyDepth 2  </VirtualHost>  <VirtualHost 169.254.48.101:443>  SSLEngine On  SSLCertificateFile "C:/OpenSSL/keyStore/ApacheServer.cer"  SSLCertificateKeyFile "C:/OpenSSL/keyStore/ApacheServer.key"  SSLCACertificateFile "C:/OpenSSL/keyStore/ca.cer"  SSLVerifyClient require  SSLOptions +StdEnvVars +StrictRequire +ExportCertData  SSLVerifyDepth 2  </VirtualHost> |

### PHP configuration

The PHP (Hypertext Preprocessor) is a programming language that allows creating web pages with dynamic content. It has to be configured to run with Apache server. Following the ‘php.ini’ file that contains all configuration of PHP for this deployment.

|  |  |
| --- | --- |
| [PHP]  engine = On  zend.ze1\_compatibility\_mode = Off  short\_open\_tag = Off  asp\_tags = Off  precision = 14  y2k\_compliance = On  output\_buffering = 4096  zlib.output\_compression = Off  implicit\_flush = Off  unserialize\_callback\_func=  serialize\_precision = 100  allow\_call\_time\_pass\_reference = Off  safe\_mode = Off  safe\_mode\_gid = Off  safe\_mode\_include\_dir =  safe\_mode\_exec\_dir =  safe\_mode\_allowed\_env\_vars = PHP\_  safe\_mode\_protected\_env\_vars = LD\_LIBRARY\_PATH  disable\_functions =  disable\_classes =  expose\_php = On  max\_execution\_time = 30  max\_input\_time = 60  memory\_limit = 128M  error\_reporting = E\_ALL  display\_errors = Off  display\_startup\_errors = Off  log\_errors = On  log\_errors\_max\_len = 1024  ignore\_repeated\_errors = Off  ignore\_repeated\_source = Off  report\_memleaks = On  track\_errors = Off  variables\_order = "GPCS"  register\_globals = Off  register\_long\_arrays = Off  register\_argc\_argv = Off  auto\_globals\_jit = On  post\_max\_size = 8M  magic\_quotes\_gpc = Off  magic\_quotes\_runtime = Off  magic\_quotes\_sybase = Off  auto\_prepend\_file =  auto\_append\_file =  default\_mimetype = "text/html"  extension\_dir = "C:/Program Files/Apache Software Foundation/php/ext"  enable\_dl = On  file\_uploads = On  upload\_max\_filesize = 2M  allow\_url\_fopen = On  allow\_url\_include = Off  default\_socket\_timeout = 60  extension=php\_gd2.dll  extension=php\_gettext.dll  extension=php\_ldap.dll  extension=php\_mbstring.dll  extension=php\_mysql.dll  extension=php\_mysqli.dll  extension=php\_openssl.dll  [Syslog]  define\_syslog\_variables = Off  [mail function]  SMTP = localhost  smtp\_port = 25  [SQL]  sql.safe\_mode = Off  [ODBC]  odbc.allow\_persistent = On  odbc.check\_persistent = On  odbc.max\_persistent = -1  odbc.max\_links = -1  odbc.defaultlrl = 4096  odbc.defaultbinmode = 1 | [MySQL]  mysql.allow\_persistent = On  mysql.max\_persistent = -1  mysql.max\_links = -1  mysql.default\_port =  mysql.default\_socket =  mysql.default\_host =  mysql.default\_user =  mysql.default\_password =  mysql.connect\_timeout = 60  mysql.trace\_mode = Off  [MySQLi]  mysqli.max\_links = -1  mysqli.default\_port = 3306  mysqli.default\_socket =  mysqli.default\_host =  mysqli.default\_user =  mysqli.default\_pw =  mysqli.reconnect = Off  [bcmath]  bcmath.scale = 0  [Informix]  ifx.default\_host =  ifx.default\_user =  ifx.default\_password =  ifx.allow\_persistent = On  ifx.max\_persistent = -1  ifx.max\_links = -1  ifx.textasvarchar = 0  ifx.byteasvarchar = 0  ifx.charasvarchar = 0  ifx.blobinfile = 0  ifx.nullformat = 0  [Session]  session.save\_handler = files  session.use\_cookies = 1  session.name = PHPSESSID  session.auto\_start = 0  session.cookie\_lifetime = 0  session.cookie\_path = /  session.cookie\_domain =  session.cookie\_httponly =  session.serialize\_handler = php  session.gc\_probability = 1  session.gc\_divisor = 1000  session.gc\_maxlifetime = 1440  session.bug\_compat\_42 = 0  session.bug\_compat\_warn = 1  session.referer\_check =  session.entropy\_length = 0  session.entropy\_file =  session.cache\_limiter = nocache  session.cache\_expire = 180  session.use\_trans\_sid = 0  session.hash\_function = 0  session.hash\_bits\_per\_character = 5  url\_rewriter.tags = "a=href,area=href,frame=src,input=src,form=fakeentry"  [Tidy]  tidy.clean\_output = Off  [soap]  soap.wsdl\_cache\_enabled=1  soap.wsdl\_cache\_dir="/tmp"  soap.wsdl\_cache\_ttl=86400 |

### DataBase server configuration

The DataBase server used for this project is MySQL. Following the ‘my.ini’ file that contains all configuration of MySQL server for this deployment:

|  |
| --- |
| # MySQL Server Instance Configuration File  [client]  port=3306  [mysql]  default-character-set=latin1  [mysqld]  port=3306  ssl-ca= C:/OpenSSL/keyStore/ca.cer  ssl-cert= C:/OpenSSL/keyStore/MySQLServer.cer  ssl-key= C:/OpenSSL/keyStore/MySQLServer.key  ssl-cipher= DHE-RSA-AES256-SHA:AES128-SHA  basedir="C:/Program Files/MySQL/MySQL Server 5.0/"  datadir="C:/Program Files/MySQL/MySQL Server 5.0/Data/"  default-character-set=latin1  default-storage-engine=INNODB  sql-mode="STRICT\_TRANS\_TABLES,NO\_AUTO\_CREATE\_USER,NO\_ENGINE\_SUBSTITUTION"  max\_connections=100  query\_cache\_size=0  table\_cache=256  tmp\_table\_size=9M  thread\_cache\_size=8  myisam\_max\_sort\_file\_size=100G  myisam\_sort\_buffer\_size=18M  key\_buffer\_size=11M  read\_buffer\_size=64K  read\_rnd\_buffer\_size=256K  sort\_buffer\_size=256K  innodb\_additional\_mem\_pool\_size=2M  innodb\_flush\_log\_at\_trx\_commit=1  innodb\_log\_buffer\_size=1M  innodb\_buffer\_pool\_size=18M  innodb\_log\_file\_size=10M  innodb\_thread\_concurrency=8  max\_allowed\_packet=8M |

After restarting MySQL server, we can check the new configuration by executing following querys:

|  |
| --- |
| show variables like '%ssl%';  show variables like '%allowed\_packet%'; |

To create a user that accepts just ssl connection, we have to execute the following query:

|  |
| --- |
| GRANT ALL on inse6120.\* TO 'ssluser'@'%' IDENTIFIED BY 'password' REQUIRE SSL; |

### LDAP Server configuration

The LDAP server used for this project is OpenLDAP. Following the ‘slapd.conf’ file that contains all configuration of OpenLDAP server for this deployment:

|  |
| --- |
| ucdata-path ./ucdata  include ./schema/core.schema  include ./schema/cosine.schema  include ./schema/inetorgperson.schema  include ./schema/misc.schema  include ./schema/openldap.schema  pidfile ./run/slapd.pid  argsfile ./run/slapd.args  TLSCipherSuite HIGH:MEDIUM:+SSLv2  TLSCACertificateFile "C:/OpenSSL/keyStore/ca.cer"  TLSCertificateFile "C:/OpenSSL/keyStore/LdapServer.cer"  TLSCertificateKeyFile "C:/OpenSSL/keyStore/LdapServer.key"  TLSVerifyClient never  database bdb  suffix "dc=myserver,dc=dev"  rootdn "cn=Manager,dc=myserver,dc=dev"  rootpw secret  directory ./data  index objectClass eq |

To start server listening on secure ports, we have to execute the following instruction:

|  |
| --- |
| C:\Program Files\OpenLDAP>slapd -h "ldap:/// ldaps:///636" |

There is also an important path file to create to allow PHP using SSL with LDAP:

|  |
| --- |
| C:\OpenLDAP\sysconf \ldap.conf |

The client application that allows us to easily manage LDAPServer is PHPLDAPAdmin. It’s an open source php application that look like the following screen shot:

|  |
| --- |
|  |

We can also configure this client application to connect to remote LDAP server by modifying the following file:

|  |
| --- |
| C:\Program Files\Apache Software Foundation\www\myserver.dev\public\_html\ldap\config\config.php  $ldapservers->SetValue($i,'server','name','INSE6120 LDAP Server');  $ldapservers->SetValue($i,'server','host','ldaps://LdapServer');  $ldapservers->SetValue($i,'server','auth\_type','config');  $ldapservers->SetValue($i,'login','dn','cn=Manager,dc=myserver,dc=dev');  $ldapservers->SetValue($i,'login','pass','secret'); |

### SSL/TLS validation

In each server, we did install **Wireshark** tool that allow us to sniff the traffic over the network. Like that, we could be able to check if communication is encrypted. Following screen shot of Wireshark running on Apache, OpenLDAP and MySQL:

|  |
| --- |
| Figure : Encrypted communication between User and Web Server |

|  |
| --- |
| Figure : Encrypted communication between MySQL and PHP |

|  |
| --- |
| Figure 8: Encrypted communication between LDAP and PHP |

# Size and Performance

The Secure Web Application supports all size and performance requirements that are stipulated in the software requirements specification.

# Quality

The Secure Web Application supports all quality requirements that are stipulated in the software requirements specification.