**Secure Web Application**

**SWA**

**Software Requirements Specifications**

**Team Members**

Ahmad Abuashour(6144926)

Prosenjit Sinha(9190740)

Akram Bouktab()

Rebbeca Gideon(9329935)

Contents

[1. Introduction 3](#_Toc215955121)

[1.1 Purpose 3](#_Toc215955122)

[1.2 Scope 3](#_Toc215955123)

[1.3 Definitions, acronyms, and abbreviation 3](#_Toc215955124)

[1.4 References 4](#_Toc215955125)

[1.5 Overview 4](#_Toc215955126)

[2. Overall description 5](#_Toc215955127)

[2.1 Product perspective 5](#_Toc215955128)

[2.2 Product functions 6](#_Toc215955129)

[2.3 User characteristics 7](#_Toc215955130)

[2.3.1 Clients: 7](#_Toc215955131)

[The clients can view the list of existing files, upload a new file, download or delete an existing file. 7](#_Toc215955132)

[2.3.2 Administrators: 7](#_Toc215955133)

[2.4 Constraints 7](#_Toc215955134)

[2.5 Assumptions and dependencies 8](#_Toc215955135)

[3. Specific requirements 8](#_Toc215955136)

[3.1 External interface requirements 8](#_Toc215955137)

[3.1.1 User interfaces (UI) 8](#_Toc215955138)

[3.1.2 Hardware interfaces (HI) 15](#_Toc215955139)

[3.1.3 Software interfaces (SI) 15](#_Toc215955140)

[3.1.4 Communications interfaces (CI) 15](#_Toc215955141)

[3.2 Functional requirements 16](#_Toc215955142)

[3.2.1 Authentication requirement: 16](#_Toc215955143)

[3.2.2 Operation requirement: 17](#_Toc215955144)

[3.2.3 Performance requirements 17](#_Toc215955145)

[3.3 Software system attributes 17](#_Toc215955146)

[3.3.1 Reliability 17](#_Toc215955147)

[3.3.2 Availability 17](#_Toc215955148)

[3.3.3 Security 17](#_Toc215955149)

[3.3.4 Maintainability 17](#_Toc215955150)

# Introduction

## Purpose

The purpose of this SRS is to describe the requirement needed to build a Secure Web Application (SWA). This document describes the procedure and methodologies that need to be taken to build a highly secure web application. The Web application maintains some user data in the database which can be accessed according to a user capability list. This document also specifies hardware and software requirements that are needed to deploy SWA application.

The intended audiences of the SRS are designers, programmers and testers.

## Scope

This document specifies the requirements for the following components of the SWA:

* The web server used as a central principal between user application, Database server and LDAP server.
* Database secure connectivity.
* The directory service used for storing and retrieving user information (Certificate).
* Hardware and software used for running the application.
* Client interface that is used to let the user authenticate himself to the server.

## Definitions, acronyms, and abbreviation

SWA: Secure Web Application

DER: Distinguished Encoding Rules

PEM: Privacy Enhanced Mail

CA: Certification Authority

HTTP: Hypertext Transfer Protocol

LDAP: Lightweight directory access protocol

PKCS: Public Key Cryptographic

SDS: Secure document system

SRS: Software Requirements Specifications

SSL/TLS: Secure Sockets Layer/Transport layer security

## 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 v1.1

<http://httpd.apache.org/docs> : Apache web server documentation

<http://www.php.net/docs.php> : PHP documentation

<http://dev.mysql.com/doc> : MySQL documentation

<http://ww.openldap.org/doc> : OpenLDAP documentation

**IEEE Std 830-1998**: Recommended Practice for SRS

## Overview

This software aims to build a secure web application where only authenticated users are allowed to access the service. The authentication is achieved via using digital certificate, which are issued by a central trusted certification authority. It is assumed that certificates are distributed among the users manually in a secured way. All the intermediate traffic between the principals is conducted using SSL.

The Secure web application (SWA) is comprised of three main principles. First principal is: LDAP Server, which is mainly used to authenticate the user of the system. To do this, it stores all the client certificates within it. Second principal is: web server that is considered as a central component responding all http or https request with maintaining all the authentications. Finally: Database server store all the client data along with access control list of all those data or files.

This document is an SRS that is fully described with IEEE Std 830-1998 that describes the Recommended Practice for Software Requirements Specifications.

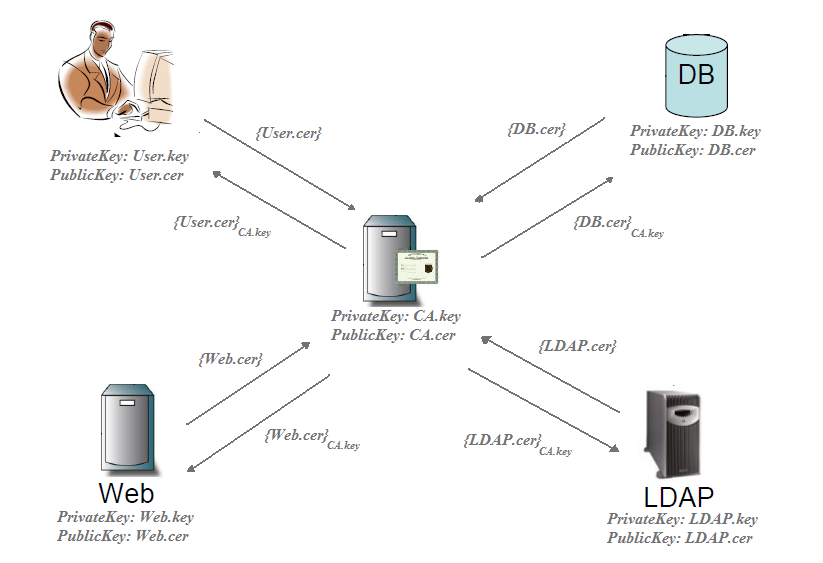
# Overall description

## Product perspective

This Web application should be based on Client-certificate authentication. Client-certificate authentication is a more secure method of authentication than either basic or form-based authentication. It uses HTTP over SSL, in which the server and, optionally, the client authenticate one another using public key certificate. *Secure Socket Layer* (SSL) provides data encryption, server authentication, message integrity, and optional client authentication for a TCP/IP connection. We can think of a *public key certificate* as the digital equivalent of a passport. It should be issued by a trusted organization, which is called a *certificate authority* (CA), and provides identification for the bearer.

If we specify client-certificate authentication, the web server will authenticate the client using the client's *X.509 certificate*, a public key certificate that conforms to a standard that is defined by X.509 Public Key Infrastructure (PKI). Before running the application that uses SSL, we must configure SSL support on the server and set up the public key certificate.

Compared to traditional public-key authentication, this method is more secure because the system checks that the user certificate was issued by a trusted CA.



## Product functions

The major function of this secure system is to access data of a remote system in a secured way. Users of the system can access the repository of the data by submitting his certificate to the web server. If he is a valid user then he can access the database. He can upload, download and delete data files. Administrator of the system also can play the same role that a normal user can play along with managing users.

## User characteristics

This application supports two types of users based on their privileges:

### Clients:

### The clients can view the list of existing files, upload a new file, download or delete an existing file.

### Administrators:

Administrator of the system can play the same role that a normal user can play. He can also manage users by creating new users with new signed certificate, deleting an existing user, managing access control list of existing files, managing capability list of existing users. He can also perform maintenance operation by checking log files.

## Constraints

The following constraints need to be carefully evaluated by the person who design the system; as these constraints will effectively limit some of the design choices.

* + Application must use relational database to store user data.
  + Application must use lightweight directory access protocol (LDAP) server to manage user certificate.
  + All communication between the principals must be encrypted using SSL.
  + All certificates that are used for secure communication should be signed by a single certification authority.
  + All servers must be run on windows platform.
  + All server hardware configuration should be upper or equal to the configuration listed below:
  + Processor: 1.5 GHZ (INTEL or INTEL compatible)
  + Memory: 1 GByte.

## Assumptions and dependencies

This Secure Web System depends on the following Open Source projects:

* Apache web server,
* MySQL database server,
* OpenLDAP ,
* PHP,
* OpenSSL.

This secure system assumes the following assumptions:

* User certificate distribution should be done manually and in a secure way.
* Web server is not vulnerable from any compromising attack.
* User certificate is installed in user end with a secure password.

# Specific requirements

## External interface requirements

### User interfaces (UI)

UI1: The user interface to the secure system.

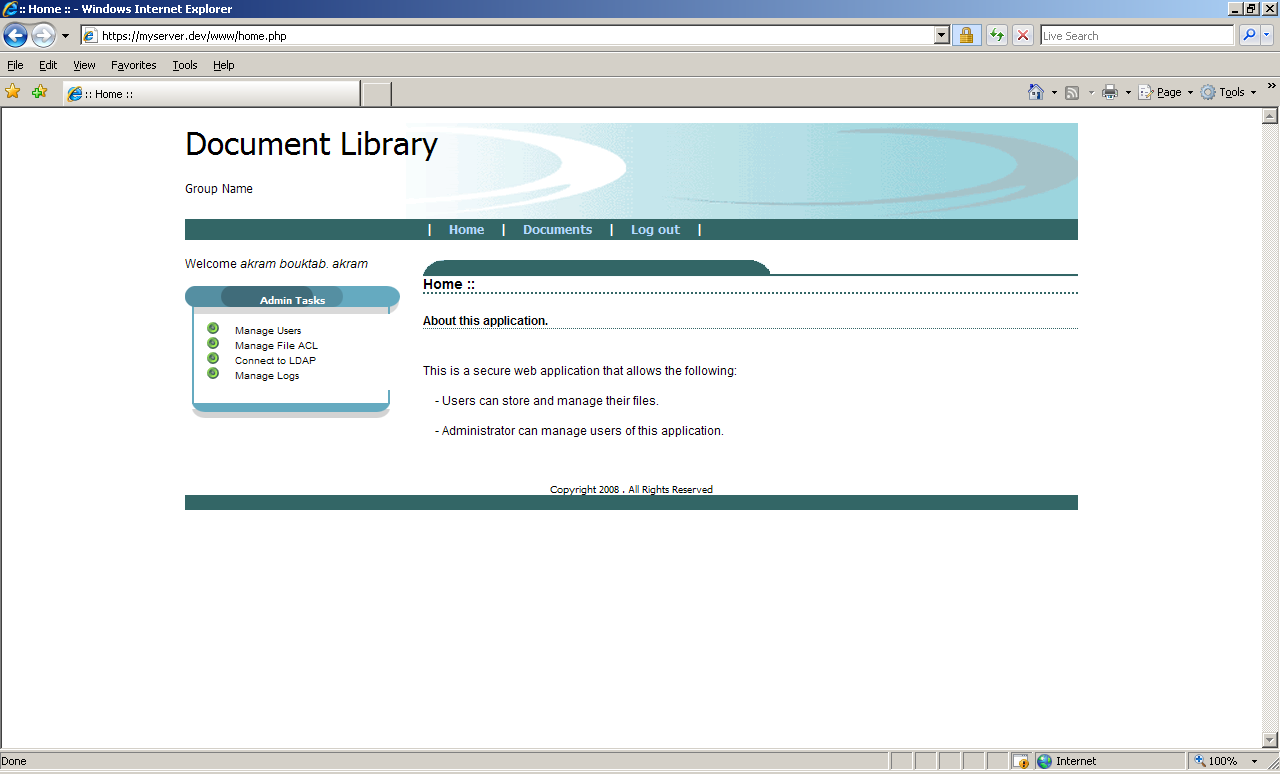


Figure : home page

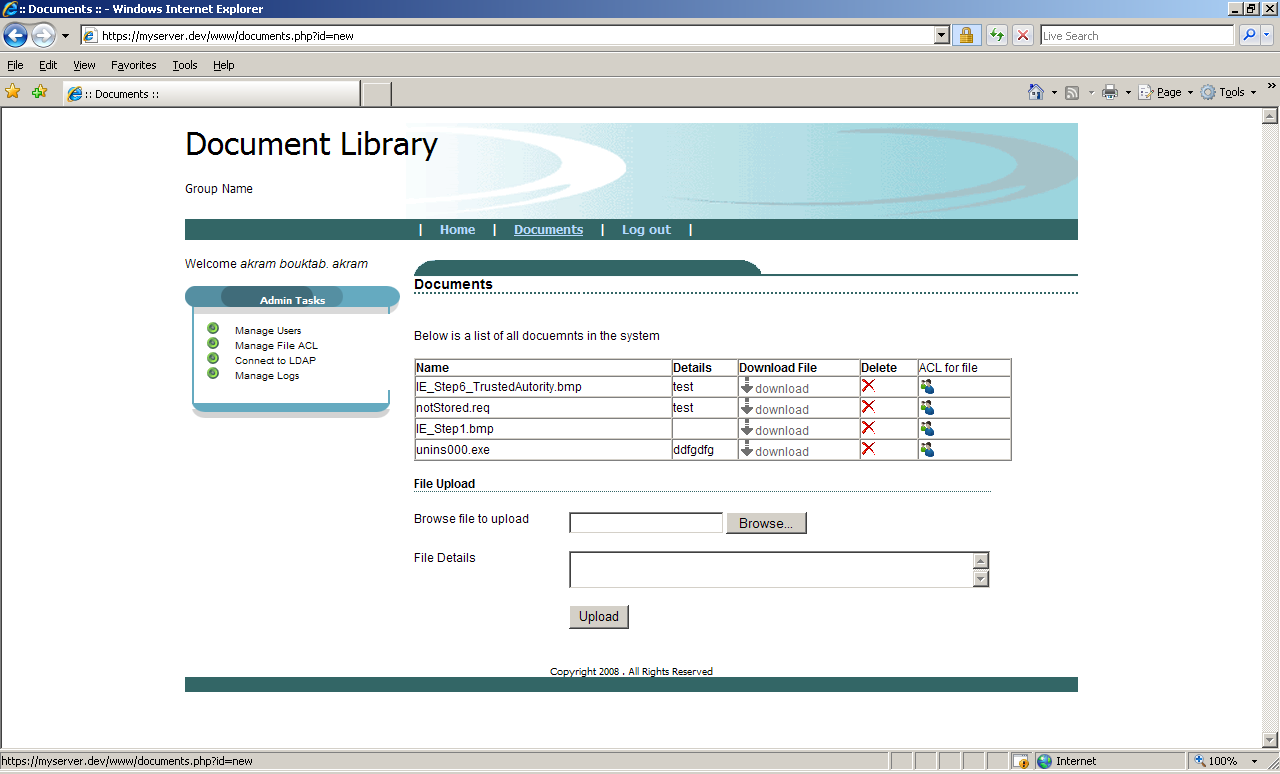


Figure : Files list page

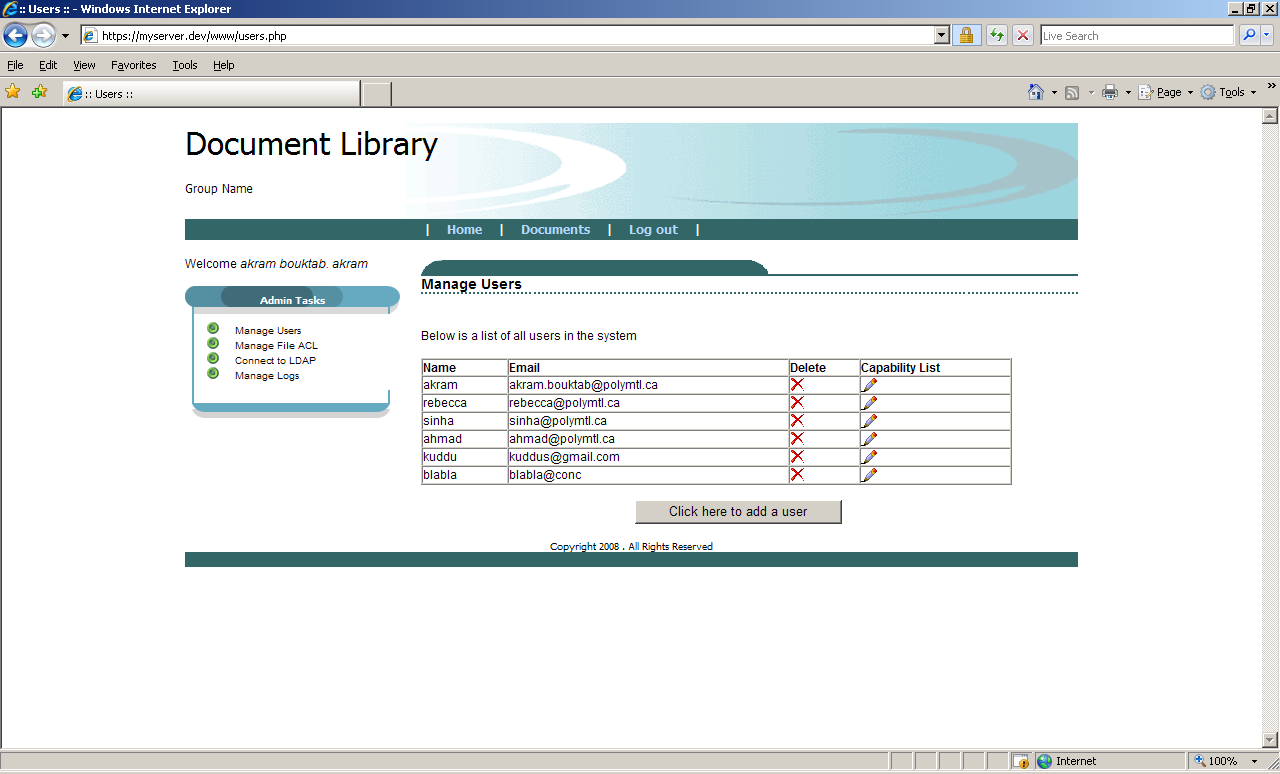


Figure : Manage users page

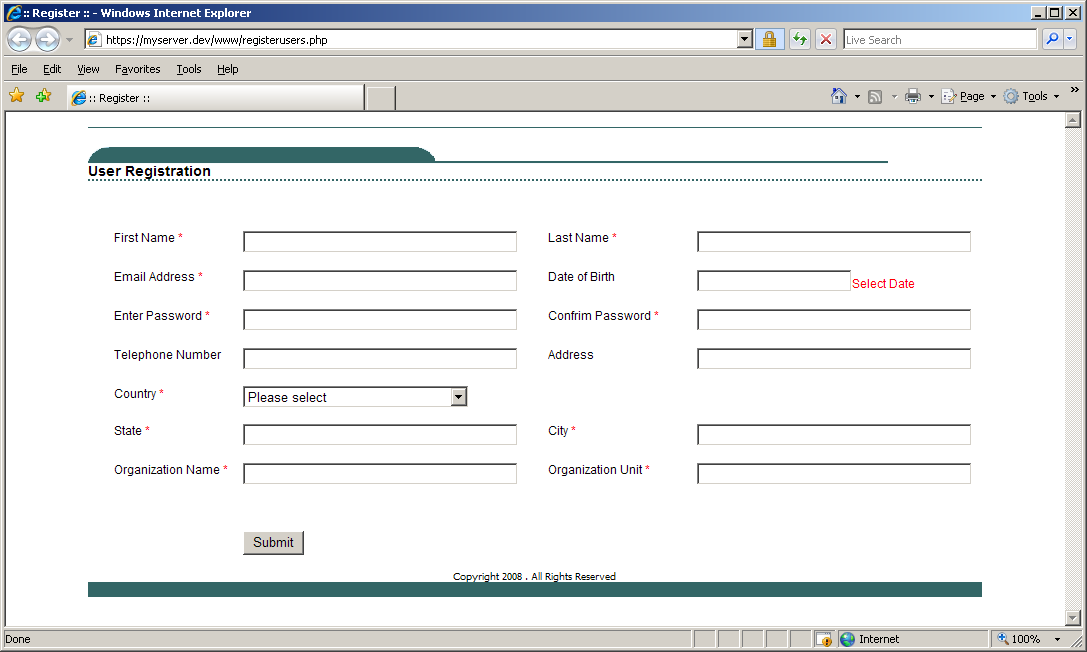


Figure : Add new user page

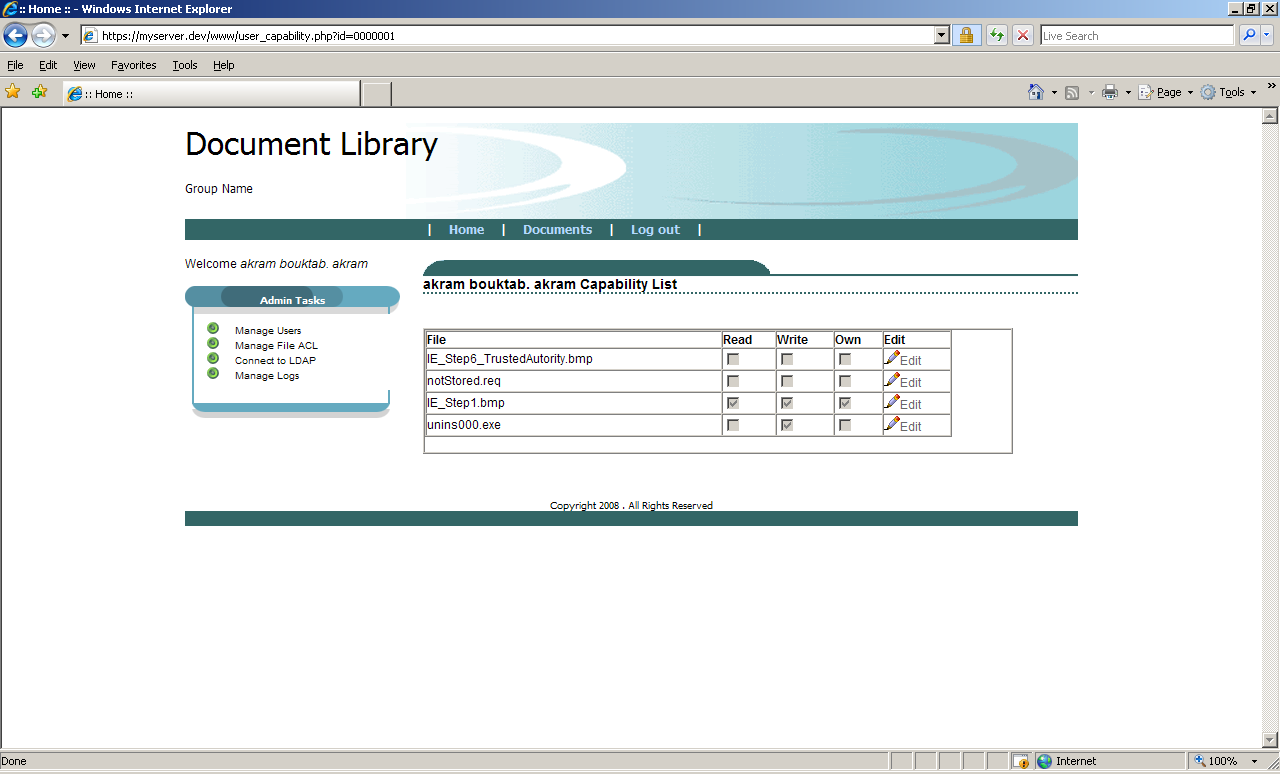


Figure : Capability list page

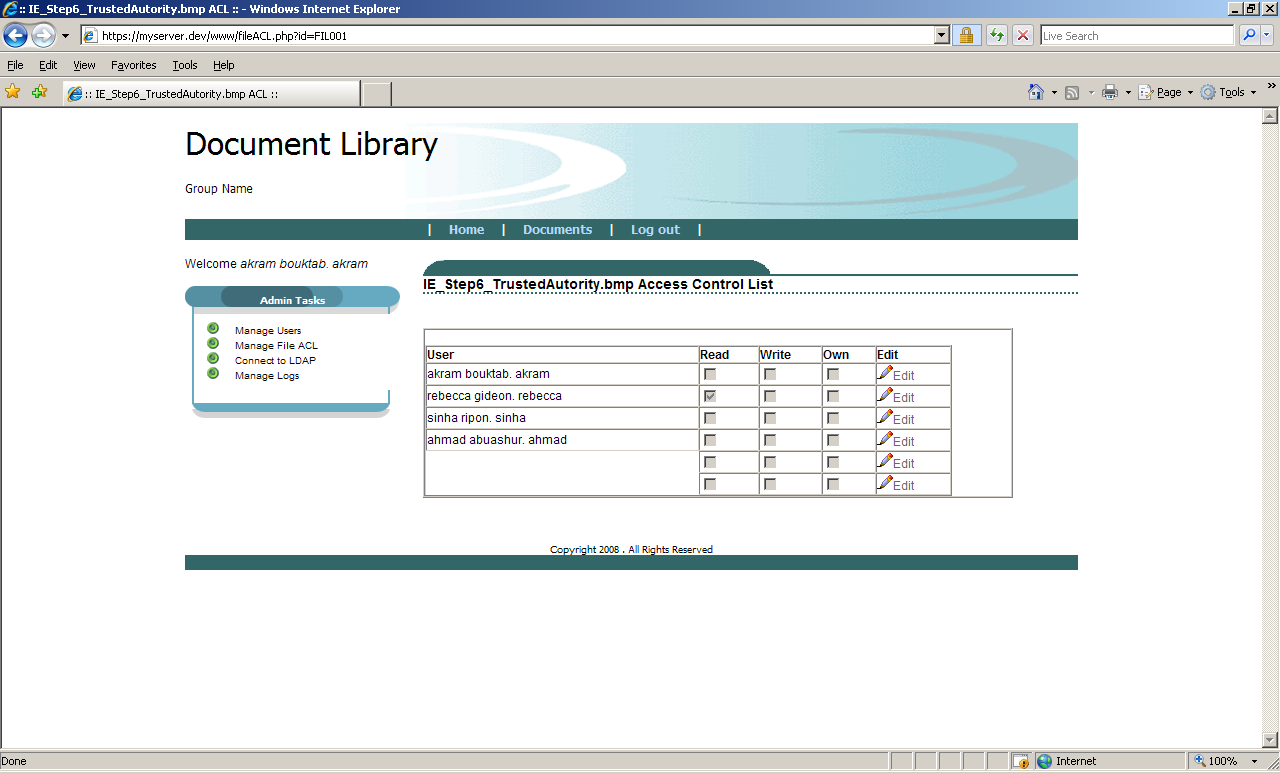


Figure : ACL page

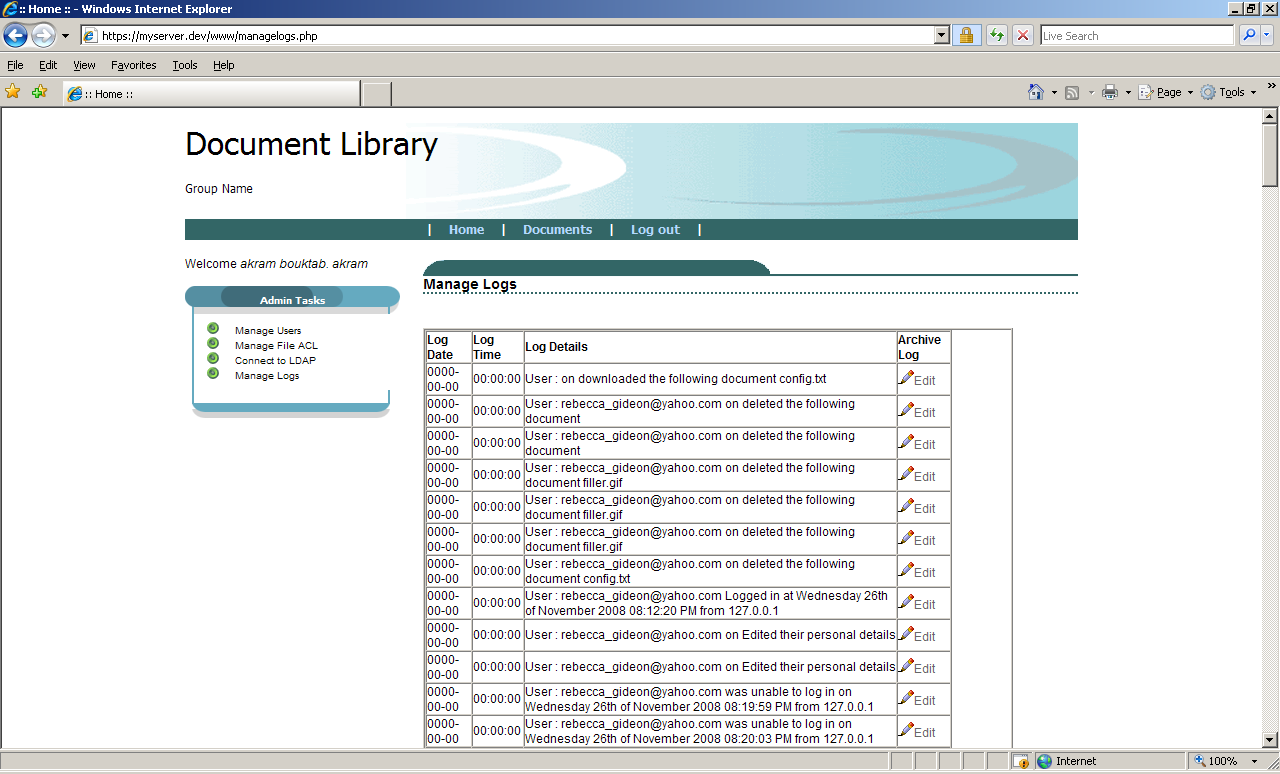


Figure : Logs page

UI2: The user can use any web browser with his certificate installed within that browser.

### Hardware interfaces (HI)

HI1: The Secure system need three different server machines whose configuration may vary depending on the user load.

HI2: The components of the Secure System must be able to run on different type of machine and brand.

### Software interfaces (SI)

SI1: The server components must be able to run on Windows XP system.

SI2: The Secure System must use MySQL as the database.

SI3: The web server must be apache web server

SI4: The LDAP server must be openLDAP.

SI5: The certificate that distributed to the users is generated by administrator using OpenSSL and should be in .PEM format and the certificate should also need to be stored in a .P12 type key store which is protected by a password.

### Communications interfaces (CI)

CI1: communication between user browser and web server should be on https to avoid any eavesdropping.

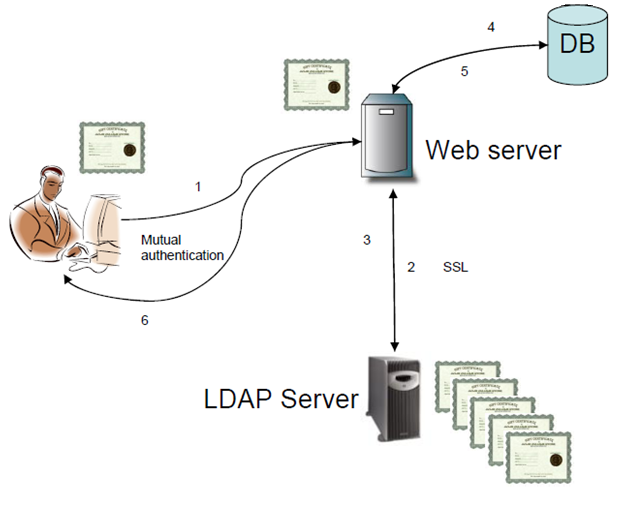
CI2: web server should need to communicate with both ldap and MYSQL database using SSL.

CI3: The authentication of principals must be based on certificate

CI4: All certificates should be provided by a common certification authority (CA).

## Functional requirements

Requirement of the Secure Web Application is mainly divided into two categories.



### Authentication requirement:

* At the beginning user will present his certificate, which is signed by a CA, to the web server. Then web server will communicate the LDAP server to validate the certificate. If the certificate is valid then the user is given permission to access the system.
* To communicate with LDAP server; web server should ask LDAP server for his valid certificate. Communication channel will be established if the certificate is valid.
* Same scenario will happen between web server and MYSQL server. Web server will ask certificate to authenticate MYSQL server and authenticate him if server is valid.

### Operation requirement:

* The clients can view the list of existing files, upload a new file, download or delete an existing file.
* Administrator of the system can play the same role that a normal user can play. He can also manage users by creating new users with new signed certificate, deleting an existing user, managing access control list of existing files, managing capability list of existing users. He can also perform maintenance operation by checking log files.

### Performance requirements

* Bandwidth of the network connection should be high enough to support upload and download of the user files. Minimum download speed should be 50kbps, and minimum upload speed should be 20kbps.
* Web server system should be run on the following specification:
* INTEL 2GHZ processor.
* 2GB Memory

## Software system attributes

### Reliability

System should be reliable considering the parameters of the centralized system.

### Availability

The Secure System must be accessible to user at any time.

### Security

All the communication between intermediate principals must be secured and encrypted to prevent the attacker to violet integrity and to prevent eavesdropping. All operation must be done by only legal users.

### Maintainability

The Secure System must declare each component clearly, in case of maintenance you can test, debug and fix each component independently, and this make it easier to maintain the code.