Cryptography project

Create an application that represents a secure repository for storing confidential documents. The application should enable document storage for a large number of users, ensuring that access to a specific document is allowed only for its owner.

Users log in to the system through a two-step process. In the first step, users need to enter the digital certificate they receive when creating their account. If the certificate is valid, the user is presented with a form to enter their username and password. After a successful login, the user can access a list of their documents through an arbitrarily implemented interface.

The application offers users the option to download existing documents and upload new documents. Each new document is divided into N segments (N≥4, randomly generated value) before being stored on the file system. Each of these segments is placed in a different directory to enhance the system's security and reduce the possibility of document theft. It's necessary to adequately protect the confidentiality and integrity of each segment so that only the user to whom the document belongs can possess it and view its content. The application should detect any unauthorized changes to stored documents and notify the user when attempting to download such documents.

The application assumes the existence of a public key infrastructure. All certificates should be issued by a Certificate Authority (CA) established before the application's operation. It is assumed that on an arbitrary location in the file system, there will be a CA certificate, a Certificate Revocation List (CRL), certificates for all users, as well as the private key of the currently logged-in user (mechanisms for key exchange are not required to be implemented). User certificates should be restricted to be used only for purposes required by the application. Additionally, the data in the certificate should be associated with the corresponding user data. User certificates are issued for a period of 6 months. Furthermore, if a user enters incorrect credentials three times during a single login, their certificate is automatically suspended, and the application displays an appropriate message. Afterward, the application offers the user the option to reactivate the certificate (if correct credentials are provided) or register a new account.