Secure Repository for Confidential Documents

Write an application that represents a secure repository for storing confidential documents. The application should allow for storing documents for a larger number of users so that access to a specific document is only allowed to its owner.

Users log in to the system in two steps. In the first step, it is necessary to enter a digital certificate that each user receives when creating an account. If the certificate is valid, the user is shown a form for entering a username and password. After a successful login, the user is provided with a list of their documents through an arbitrarily designed interface.

The application allows the user to download existing documents as well as upload new ones. Each new document is divided into N segments ($N \geq 4$, randomly generated value) before being stored in the file system, with each of these segments stored in a different directory to further increase the security of the system and reduce the possibility of document theft. It is necessary to protect the confidentiality and integrity of each segment in an appropriate way so that only the user to whom the document belongs can obtain it and see its content. The application should detect any unauthorized changes to stored documents and notify the user about them when attempting to download such documents.

The application assumes the existence of a public key infrastructure. All certificates should be issued by a CA body that is established before the application starts working. It is assumed that the CA certificate, CRL list, user certificates, and the private key of the currently logged-in user will be located at an arbitrary location in the file system (mechanisms for exchanging keys do not need to be implemented). User certificates should be restricted so that they can only be used for purposes required by the application. In addition, data in the certificate should be associated with the corresponding user data.

User certificates are issued for a period of 6 months. In addition, if a user enters incorrect credentials three times during one login, their certificate is automatically suspended, and the application displays an appropriate message. After that, the application offers the user the option to reactivate the certificate (if they enter the correct credentials) or to register a new account.