**Security requirements**

The following is a description of the security requirements that this program needs in order to run on correct way.

**Permission**: The group server needs to be on “ADMIN account” or “ADMIN group” status, in order to be able to add or delete a user. Therefore, “ADMIN group” will be the only one allowed to delete and create a user or a group. User of the system must pay attention on this procedures, otherwise the system will no run on a proper way.

**Account Verification**: In order to identify a user, he must provide his username and password.

**Unauthorized Token Issuance**: For a user to begin using the secure file server, they must be issued a token with which they can perform all the functions of the Group and File Servers. Thus, we need to protect each user’s token from anyone other than the user.

**Token Modification**: By modifying or forging tokens issued by the Group Server, a user may be able to gain access to files that would otherwise be forbidden. By changing the group information embedded in a token, a malicious user can access groups that they are not members of, which would grant unauthorized access to files belonging to those groups.

**Passive Attack**: Suppose Eve can listen to an information exchange between Alice and Bob. Even without being able to interrupt or modify the exchange, Eve can still glean enough information to perform malicious acts. If insufficient security is in place, Eve may be able to gather enough data to

* Know the contents of the exchanges;
* To impersonate Alice or Bob;
* Use offline password guessing to discover passwords or other secret information.

Eve does not need to be an active participant in a conversation to illicitly benefit from it, and thus exchanges between Alice and Bob must be kept secure. Or, to put into context of a secure file server, any exchanges between a user and any server (or even between servers) must be kept confidential if proper security is to be maintained.