A security system

Goals and objectives

1) Identifies a person
2) Controls access to authorized persons
3) User selects his/her own password
4) Controls access to individual files (including OBJ files)
5) Integrates with current directory access system.
6) Integral to Comet; applies to all applications including Reporter, View Manager, DB Manager, Comet Explorer

Internals

1) Controlled by a file containing one record for each user. A user profile file.
2) Only the system administrator can maintain this file.
3) When the file is created a record identified with the magic word "ADMINSTRATOR" is created.
4) When the file is created the installer must establish the password for the Administrator.
5) Passwords are encrypted when stored in the file.
6) Only the administrator can change her own password.
7) The administrator can remove passwords in the file, but can not establish new passwords for users.
8) When a user logs into the Comet system the user enters her user-name, password and directory access logon (key to the current PASSWORD file.)
9) When a user logons onto the system and a user record with a blank password exists, the user will be prompted to select a new password.
10) When there is only one directory access logon in the user's profile record the system will not prompt for the directory access logon but will automatically use the only one allowed.
11) A user can be simultaneously logged in more than one time, but all the logins must be from the same machine ID meaning these are multiple concurrent sessions on one workstation.
12) The user profile record contains:
    a. User name
    b. Encrypted password
    c. A list of twenty directory access logon keys
    d. Two arrays of 300 elements in each:
        i. Array 1 is a list of file names; all valid Comet file types are allowed including object files, D00 files, V00 files, etc.
        ii. Array 2 specifies the rights the user has to the file: Read, Write, Erase, Create, Rename

13) The system default is all rights; when the user accesses a file that is not specified in that user's profile record the system acts as though the user has all rights. The profile record serves to restrict access; it does not allow access.

Open issues

1) Should the user profile file have a pre-determined name or should the installer select the name as happens now with the current PASSWORD file?
2) Should other information be included in the profile record –
    a. Which printers the user is authorized to access?
    b. Whether the user is, [can be] a local user, a remote CometAnywhere user, or either?
    c. Should there be a date created field in the profile record?
    d. Should there be an Administrator equivalent?
    e. User's full name?
    f. User's department?
    g. User's phone extension?
    h. Email address?
    i. IM name?
    j. Terminal ID when user is logged onto system
    k. Last log in date and time
    l. Last log off date and time
3) How do users log off? Should Comet dump users off after a specified period of inactivity?