bcc	title	prefix/class-number.revision
	The Account and User Directories	AUD/W-7.1

checked	authors	approval date	revision date
Bobby W Sampson	Larry Barnes	10/29/69	10/28/69
checked		classification	
Claire Thuf		Working Paper	
approved		distribution	pages
Mef	Larry L Barnes	Company Private	7

ABSTRACT and CONTENTS

This document describes the account and user directories used for name conversions by the utility. It also describes the user profile and standard operations on it.

1. Access Control for the Account and User Directories

We distinguish access by dividing users into one of four categories:

1) System Owner - one user,
2) Group Owner - one user per group,
3) Account Owner - one user per account, and
4) Normal - all other users.

As will be explained in a document on resource control, convincing the system that you are a user in one of the first three categories gives you control over users in higher-numbered ones. This control is implemented through the use of the user number as an access key to unlock appropriately privileged files. Each group has either an Account Directory (AD) or (for small groups) a User Directory (UD). The files are owned by the proper Group Owner. Each utility system will execute in a sub-process one of whose access keys is the user number of the appropriate Group Owner. This convention gives it access to all files it needs to control access to its own resources.

The names of the groups, accounts, and users are highly confidential. In keeping with the policy of protecting groups from each other, but not protecting a group from itself, we will allow the group to read and modify its AUD as it pleases. However our standard utility system is required to protect a group's interests in a manner similar to basic system protection.

A group which operates a service bureau must protect accounts from each other while allowing the Account Owner to modify his User Directory (UD). Thus the UDs will be implemented in an analoguous manner. Some groups (such as BCC) may want to allow normal users to operate without account boundaries. In this case the account directory is eliminated and the group uses only a user directory.

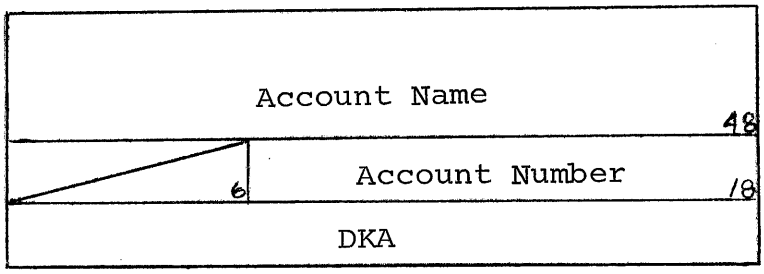
2. Format of Account and User Directories

The Account Directory (AD) is a file belonging to the group. It is limited to n (presently unspecified) pages so that it can be put into the map conveniently during entering. It consists of

a) A header, which contains a lock work. If the lock word is zero, the AD is unlocked. If it is negative, the AD is being written. Otherwise it contains a count of the number of processes reading the AD.

A standard time-out procedure will be used to handle locking of the file.

b) A series of entries of the form



The account Name is 6 8-bit characters. Only those preceding the first blank are significant to ENTER. The Account Number is that of the Account Owner (AO), and together with DKA serves to specify his MIB.

In the AO's MIB is a file called USER-DIRECTORY (UD) which contains information about the users in that account. This information is stored as a series of user profiles (UP). For single-account groups, there is no AD.

A header contains lock information similar to that on AD and a table which contains the locations of all the UPs, in no particular order.

A UP is a collection of items which are triples of the form

< item name, access flags, item value >

The item name and value are strings of less than 15 and 480 (8-bit) bytes, respectively. The first 16 bits of the user entry (UE) gives the length of the name and value and the access flags:

AR - readable by anyone in the account

UW - writeable by the user

CP - copy item into process made table at login.

The AO can read and write all the items. Authority to write implies authority to delete. New items may be added by the user or the AO provided the names do not conflict with items already present. AR and CP may be set or cleared by the user, UW only by the AO.

Every UE contains certain standard items and may contain others which are interpreted by the system in a standard way if they appear. The required standard items are

Item Name	Access Flag	Meaning
N	AR,CP	the user's name
#	AR,CP	the user's number
D	AR,CP	DKA for the user's MIB.

The optional standard items are

Item Name	Access Flag	Meaning
R		the resource table for the user. See RESRC/ for the format of this table. If this is missing the user cannot enter
P	UW	password
ED	AR,UW	Edit conventions
FS	AR,UW	File Search
CS	AR,UW	Command Search
ML	AR,UW	Mail present

3. Operations on the AUD

The normal operations on the AUD are to convert a user name to a user number and back again. By restricting the search to a single UD, the operation becomes relatively unprivileged. In addition to these operations there will be a general editing program for changing the ADs and UDs. This program is discussed in the forthcoming document on resource control.

Note that it is the user name that is the privileged information in a user directory, not the user number. Thus we lose no protection in allowing an Account Owner to add to his UD the names and user numbers of known users who are not in his account or group. There should be no way in which he can use the system to obtain this information however. We assume that individuals wishing to share files will exchange their names and user numbers to permit symbolic access to the MIBs. Among these extra names will be "BCC" for the MIB of our public proprietary programs, and the name of a similar MIB for the group.

User profiles may be accessed by

user name

user number

index in the table in the header of the UD

To this end the first two arguments of the operation on UP's an

INTEGER E, STRING S

and are interpreted as follows:

if E < Ø it is an index in the header table

if E > Ø it is a user number

if E = Ø S is a user name

The operations fail if the specified entry does not exist.

STRING FUNCTION READ'ITEM (E, STRING S, N, V) looks for an item with name = N. If it finds one, it appends its value to V and returns the resulting string. Otherwise it fails.

STRING FUNCTION READ'ITEM N (E, STRING S, INTEGER N, STRING V) is just like READ 'ITEM except that the Nth item is read,

FUNCTION SET'ITEM (E,STRING S, N, V) looks for an item with name = N. If it finds one, it sets the value to V. If it does not find one, it creates one. This operation can fail in various ways if access restrictions of section 2 are not observed.

FUNCTION SET'ACCESS (E, STRING S, N, INTEGER ON, OFF) looks for an item with name = N. If it is found the access flags specified by ON are turned on, and the ones specified by OFF are turned off. They are coded: AR = bit 23, UW = bit 22, CP = bit 21. If OFF = -1 the item is deleted.

bcc	title	prefix/class-number.revision
	THE ACCOUNT-USER DIRECTORY	AUD/W-7

checked	authors	approval date / revision date
Robert W Sansom	Larry L. Barnes	
checked	Larry L Barnes	classification: Working Paper
approved: Mel		distribution: Company Private / pages

ABSTRACT and CONTENTS

This document describes the user directory files for implementing the file-naming system. Particular attention is paid to conversion between user names and numbers. This document does not cover the accounting directories.

1. Access Control for the Account-User Directory

We distinguish access by dividing users into one of four categories:

1) System Owner - one user,
2) Group Owner - one user per group,
3) Account Owner - one user per account, and
4) Normal - all other users.

As will be explained in a document on resource control, convicing the system that you are a user in one of the first three categories gives you control over users in higher-numbered ones. This control is implemented through the use of the user number as an access key to unlock appropriately privileged files. Each group has an Account-User Directory (AUD). The file is owned by the System Owner and is read-write accessible to the proper Group Owner. Each utility system will execute in a sub-process whose user number is the appropriate Group Owner. This convention gives it access to all files it needs to control access to its own resources.

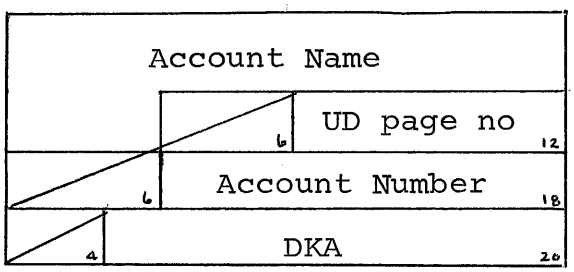
The names of the groups, accounts, and users are highly confidential. In keeping with the policy of protecting groups from each other, but not protecting a group from itself, we will allow the group to read and modify its AUD as it pleases. However our standard utility system is required to protect a group's interests in a manner similar to basic system protection.

A group which operates a service bureau must protect accounts from each other while allowing the Account Owner to modify his User Directory (UD). While the UDs can be implemented in an analoguous manner, some groups (such as BCC) may want to allow normal users to operate across account boundaries. Thus we have chosen a format for the AUD which allows both modes of operation.

2. Format of the Account-User Directory

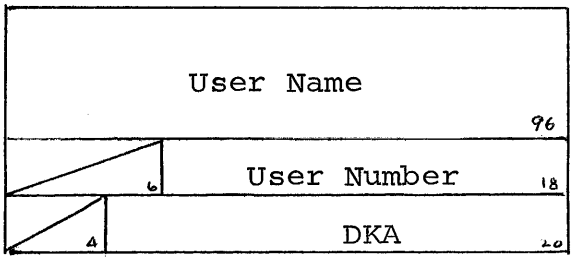
The Account-User Directory (AUD) consists of an Account Directory (AD) and several User Directories (UDs). The AD and each UD are allocated one page per directory. During the Enter procedure the utility will put the proper UD page into its map for use in file-naming operations.

The Account Directory consists of entries in the following format.



The Account Name is five six-bit characters - a letter followed by four digits. The User Directory page number is stored in the last twelve bits of the name. The Account Number and DKA field identify the MIB of the Account Owner. The first word of the AD entry is zero if the entry is not in use.

The User Directory has a similar structure.



The User Name is a sixteen character name with no embedded blanks. The User Number and DKA identify the user's MIB.

3. Operations on the AUD

The normal operations on the AUD are to convert a user name to a user number and back again. By restricting the search to an account UD, the operation becomes relatively unprivileged. In addition to these operations there will be a general editing program for changing the AUD and the resource tables, etc. This program is discussed in the forthcoming document on resource control.

Note that it is the user name that is the privileged information in a user directory, not the user number. Thus we lose no protection in allowing an Account Owner to add to his UD the names and user numbers of known users who are not in his account or group. There should be no way in which he can use the system to obtain this information, however. We assume that individuals wishing to share files will exchange their names and user numbers to permit symbolic access to the MIBs. Among these extra names will be "BCC" for the MIB of our public proprietary programs, and the name of a similar MIB for the group.