acf2® MVS

Summary of Enhancements for acf2/MVS Release 4.0

acf2®

The Access Control Facility

CHANGE SUMMARY

for

acf2/MVS Release 4.1

Base Document Dated: January 31, 1986

Doc. Nr. AMG4039-01

TABLE OF CONTENTS

CHANGE SUMMARY FOR ACF2/MVS RELEASE 4.1

acf2/MVS Release 4.1 includes many new features which increase an installation's security, provide increased efficiency for security administrators, simplify product installation and maintenance, and reduce system overhead.

A brief description of each new Release 4.1 enhancement, grouped by general function category, is included in this document.

Release 4.1 also includes a significant amount of maintenance for the acf2/MVS product. The last chapter in this document lists the SKK System Tracking and Reporting (STAR) number of each maintenance update incorporated in Release 4.1.

Only one of these AUTHSUPx bit fields may be turned on in a user's Logonid record. When an AUTHSUPx field is on, acf2/MVS passes control to an installation defined user authentication exit program only after the standard ACF2 system access validation is performed (e.g., Logonid, password, shift, source).

* Each AUTHSUPx bit field is associated with an installation defined user authentication exit program (see the description of the new AUTHEXIT global system options record below). An exit program can implement a software algorithm that prompts the user for additional information. Alternatively, the exit program can interface between ACF2 and a hardware device such as a magnetic card reader or "smart card".

* Extended User Authentication programs are defined through a new global system options (GSO) record called AUTHEXIT. Each AUTHEXIT record names the program to be called when a user has the associated bit field on in his Logonid record. Up to eight different Extended User Authentication programs can be active at one installation. However, each individual user can be associated with only one Extended User Authentication program.

* The new APPLDEF global system options (GSO) record allows the installation to optionally define the content and format for an associated class of Infostorage records. APPLDEF also allows user validation information to be stored on the ACF2 Infostorage database as IDENTITY records. There are many benefits to storing the information on the ACF2 Infostorage database:

  - The unique ACF2 one-way encryption algorithm can be used to encrypt information in each IDENTITY record.

  - Standard ACF2 commands can be used to maintain the IDENTITY records.

  - ACF2 database recovery facilities ensure that all information is restorable in case of database failure.

  - When IDENTITY records are created or changed, ACF2 reports identify the user who made the change, type of change, and date/time of the change.

* A set of commands (LIST, CHANGE, INSERT, DELETE, and REFRESH) is provided to maintain the AUTHEXIT and APPLDEF global system options records. A similar set of commands is provided to maintain IDENTITY records.

* The ACF2 Invalid Password/Authority Log (ACFRPTPW) shows all unauthorized access attempts that occur during Extended User Authentication validation.

Note that the access key number is displayed only during the first system access with NOTE #9 active. For subsequent access validations, only the authorization code number is displayed. For example:

<u>First TSO Logon with NOTE #9 Support</u>

```
logon user1234
ACF82004 ACF2, ENTER PASSWORD: <entered non-display>
ACFEA150 ACF2, YOUR NEW ACCESS KEY NUMBER IS 14
ACFEA151 ACF2, PERFORM ADDITION OF ACCESS KEY TO AUTHORIZATION PROMPT
```

In the above example, the access key number 14 is randomly generated (message ACFEA150). The operation USER1234 must perform is addition (message ACFEA151).

<u>Subsequent TSO Logons with NOTE #9 Support</u>

```
logon user1234
ACF82004 ACF2, ENTER PASSWORD: <entered non-display>
ACFEA155 ACF2, ENTER AUTHORIZATION CODE FOR 26 -  <entered non-display>
```

In the above example, only the ACFEA155 message prompt is issued. USER1234 must remember both his access key number and the operation he must perform. Note also that a new authorization code number is randomly generated at each system access. To access the system, USER1234 must add 14 to 26 (message ACFEA155) and enter 40 in response to the ACFEA155 message.

As distributed, NOTE #9 allows the user <u>one attempt</u> to enter the correct access key number. Invalid attempts are recorded via SMF for reporting on the ACF2 Invalid Password/Authority Log (ACFRPTPW). A Write-To-Operator (WTO) message is also sent to the security console when a system access request is denied.

By default, each access key number is valid for only ten system accesses. After ten accesses, the addition or subtraction process is randomly reassigned and a new access key number is generated. This feature helps prevent users from defining a program function (PF) key with their access key number. In addition, a randomly assigned access key discourages users from programatically determining the access key value.

The following chart illustrates the different data types versus various erasure mechanisms:

E R A S U R E   M E C H A N I S M S

DATA TYPE	JCL	SVC99	ACF2 Utilities	AUTOERAS Automatic Erase
VSAM	U	I	U	S
Non-VSAM	I	I	U(ACF2)	S
Temporary Non-VIO	I	I	U(ACF2)	S
VIO	S	S	S	S

where:

I = impossible
U = user action required
U(ACF2) = possible with user-invoked ACF2 utilities
S = action automatically taken by ACF2 system with AUTOERAS turned on

Activating the Automatic Erase Feature

The Automatic Erase feature is controlled via the AUTOERAS global system options record:

```
AUTOERAS NON-VSAM/NONON-VSAM
         VSAM/NOVSAM
         VOLS(volmask1,...,volmask255)
```

NON-VSAM/NONON-VSAM - specifies whether or not acf2/MVS will automatically erase non-VSAM datasets before releasing the space for future use. The non-VSAM erase is invoked via JCL disposition processing, dynamic unallocation (SVC99), a system utility (IEHPROGM), or a user program (SCRATCH). The default is NONON-VSAM which deactivates Automatic Erase for non-VSAM datasets. See also the VOLS description below.

TS73780 - "CONTROL(TSO)" SETTING SIMPLIFIES RECORD REVIEW

A new "SET CONTROL(TSO)" setting has been added in Release 4.1. This command setting allows the installation to list and delete TSO full-screen logon data records that reside on the ACF2 Infostorage Database.

When the ACF2 TSO full-screen logon support is activated for an individual user via the TSOFSCRN bit in the Logonid record, the user receives a logon screen at TSO logon time. The logon screen contains the default values from the Logonid record for region size, procedure name, account number, etc. If the user is permitted to change any of the default values, the changed values can be saved on the ACF2 Infostorage Database. The next time the user logs on, the Infostorage record is retrieved and the values previously stored in the record are inserted into the appropriate full-screen areas.

Under Release 4.1, the administrator can use the new "SET CONTROL(TSO)" setting to list a user's full-screen logon Infostorage record. For example:

```
acf
set control(tso)
list lllllll  (where lllllll is the user's Logonid)
  .
  .
  .
```

If required, the DELETE subcommand can be used to remove a record from the Infostorage Database.

TS73873 - LOGONID RECORD "IF" OPTION EXPANDED

Release 4.1 has added new flexibility to the 'IF(attribute-list)' option for processing Logonid records via the ACF command. The new IF option allows the administrator to quickly display, change, or delete Logonid records that match a specific criterion.

In the example below, all Logonid records that have both the CICS and IDMS authorization bit fields turned on are displayed:

```
acf
set lid
list if(cics,idms)
```

Note that the attribute-list is processed as an AND condition. When multiple bit fields are specified, all cited bit fields must be turned on. You can also specify the negative form. In the next example, all Logonid records that do not contain the TESTCICS authorization bit field turned on are changed:

TS73941 - UADS TO ACF2 LOGONID RECORD CONVERSION PROGRAM

Release 4.1 includes a new utility program, called ACFUADS, that converts SYS1.UADS entries into ACF2 Logonid records. ACFUADS is very easy to use and provides installations with a flexible and efficient means to fully migrate from SYS1.UADS to ACF2 Logonid records. Use of ACF2 Logonid records reduces both administrative and system overhead.

ACFUADS Utility Creates ACF INSERT Subcommand Statements

ACFUADS reads the SYS1.UADS dataset, creating an ACF INSERT subcommand statement for each SYS1.UADS member. By default, the SYS1.UADS fields listed below are converted to ACF INSERT subcommand statements. The related applicable ACF2 Logonid record field names are shown in parenthesis.

Converted UADS Fields

UADSUSER (LID)	USATRO1 (ACCTPRIV)	UADSPPWD (PASSWORD)
UADSINST (ATTR2)	UADSDEST (DFT-DEST)	UPTPFX (DFT-PFX)
UADSSOUT (DFT-SOUT)	UADSSUBC (DFT-SUBC)	UADSSUBH (DFT-SUBH)
UADSSUBM (DFT-SUBM)	USATRO2 (JCL)	UADSMAIL (MAIL)
UADSNOTC (NOTICES)	USATROO (OPERATOR)	USATRO4 (RECOVER)
UADSANUM (TSOACC)	UADSRNAM (TSOPROC)	UADSRBA (TSORBA)
UADSR512 (TSORGN)	UADSOMAX (TSOSIZE)	UADSUNAM (TSOUNIT)
USATRO3 (MOUNT)		

If one of the above fields is not defined in a particular SYS1.UADS member, ACFUADS does not include that field in the resultant ACF INSERT subcommand statement for that userid.

Other ACFUADS Options

ACFUADS accepts the following additional control options via the SYSIN input file:

* A set of ACF2 Logonid record field names and values that override the corresponding SYS1.UADS field values. For example, if the installation wants all ACF2 Logonid records to contain the JCL and MAIL attributes, then "JCL MAIL" can be specified as SYSIN input.

* An "ADD" parameter that specifies additional ACF2 Logonid record fields and values to be included on every ACF INSERT subcommand statement. For example, if the installation wants every converted Logonid record to include the JCL and CICS attributes, an "ADD(JCL,CICS)" statement can be included in the SYSIN input. Any number of ADD statements can be included.

```
@CFDE  PETRACE,LIDPAFLG,BIT,
             AUTH=PEISO,ALTER=ALL,
             LIST=ALL,FLAGS=NULL,
             BITMAP=LIDPETRC,PRTN=3,RRTN=3,GROUP=2
```

TS79845 - ACF2/IDMS SUPPORTS SIGNON PROFILE AND IDD SECURITY

Release 4.1 includes two major enhancements to the ACF2/IDMS interface: PROFILE CLIST support at IDMS signon time; and, ability to specify IDMS security class codes in a user's ACF2 Logonid record.

Signon Profile Field Added to the Logonid Record

The name of an IDMS signon PROFILE CLIST can be specified in an IDMS user's Logonid record. This enhancement allows the standard SKK-supplied ACF2/IDMS signon program to automatically initiate PROFILE CLIST execution, which eliminates the need for a user to initiate the CLIST manually. When a PROFILE name is present in a user's Logonid record, the CLIST is executed after standard ACF2 signon validation completes. The new Logonid record field name for the PROFILE CLIST name is IDMSPROF.

Integrated Data Dictionary Support

Release 4.1 of the ACF2/IDMS product allows the security class codes, which are normally defined in the IDMS Integrated Data Dictionary (IDD), to be stored in a user's Logonid record. When this feature is implemented, the ACF2 Logonid database can contain the IDD security class codes for each user. During user signon to IDMS, the security class codes are retrieved from the Logonid record and made available for IDMS security class checking. ACF2 support for IDD helps make administration of an ACF2-controlled IDMS system more efficient because all security related information about an IDMS user can now be centralized in the ACF2 Logonid database.

TS73768 - PROMPT AND TRIM OPERANDS ADDED TO @CFDE MACRO

An additional two new operands have been added to the @CFDE macro: PROMPT and TRIM.

PROMPT Operand

PROMPT is valid for any "valued" field and is useful for fields where sensitive information, such as user password, will be entered into the Logonid record. For example, the @CFDE macro for the PASSWORD field includes PROMPT=YES. Therefore, the user can use the ACF command to enter the password either directly (as before) or in a non-display, protected field (by not specifying the value on input and waiting for the prompt).

```
READY
acf
change user1234 password < PASSWORD VALUE NOT INCLUDED >
ENTER PASSWORD ________ < ACF2 PROMPTS FOR THE PASSWORD ALLOWING
                          IT TO BE ENTERED IN A NON-DISPLAY FIELD>
```

In the SKK-supplied ACFFDR, the PROMPT=YES operand has been added to the @CFDE macro for the PASSWORD field.

TRIM Operand

TRIM is valid for both hex-type and character-type Logonid record fields. When TRIM=YES, all trailing blanks are removed from character-type fields when the field is displayed. Similarly, trailing zeroes are removed from hex-type fields when TRIM=YES. The default is TRIM=YES, providing compatibility with earlier releases.

TS76575 - @CFDE MACROS FOR TSORBA AND ACC-SRCE

The @CFDE macro default values for the TSORBA and ACC-SRCE Logonid record fields are changed.

The @CFDE for TSORBA now includes FLAGS=NEVER so that the field name and content of TSORBA is never displayed when a Logonid record is listed.

The @CFDE for ACC-SRCE now includes FLAGS=NULL so that the field name and content of ACC-SRCE is displayed only when a source value is present.

ENHANCEMENTS TO THE ACF2/CICS SECURITY SUBSYSTEM

ACF2/CICS Release 4.1 includes many enhancements that simplify the implementation and administration of CICS security controls. In addition, ACF2/CICS Release 4.1 uses less storage and consumes less CPU-time. Enhancements in ACF2/CICS Release 4.1 include:

* Expanded version of the ACF2/CICS Master Terminal Transaction (ACFM). Many new functions have been added to ACFM to help the CICS administrator fine tune ACF2/CICS to achieve optimum performance and minimize storage requirements.

* Resource rules can now be decompiled, edited, compiled, and stored via the new Resource Rule (RM) function of the ACFM transaction. With the addition of RM, all major ACF2/CICS security controls can now be maintained directly through ACF2/CICS.

* A new utility program, called ACFAESTC, converts the CICS Signon Table (DFHSNT) entries into ACF2 Logonid record format. See TS75889 for more details about this new utility.

* The ACF2/CICS parameter options are expanded and reorganized. One of these new options, called ACFM, allows each individual function of the ACFM transaction to be secured. Security can be implemented for all ACFM functions or selected functions. Authorized personnel can also dynamically activate or deactivate security for each function.

* Internal ACF2/CICS management modules are enhanced.

change a resource rule, the administrator simply executes the RM function to obtain the rule set. After editing, the administrator can store the rule set, if desired, and rebuild the directory to immediately activate the revised rule set. Time is saved because the administrator performs the entire rule change process through CICS (no need to logon to another time-sharing application such as TSO).

* SC - accepts a terminal identification and displays:

  - the contents of the rule cache for each resource accessed through the terminal

  - each resource type (such as TRAN, FILE, PROGRAM, etc.) present in the cache

  - the name of the resource that was accessed from the terminal (such as PROGRAMA)

  - the type of resource access request made (such as read, add, update, or delete)

* SG - displays statistics showing the actual number of acf2/MVS interactions with ACF2/CICS. This includes:

  - the number of currently signed-on users that were actually validated by ACF2/CICS

  - the total number of signons and signoffs processed by ACF2/CICS

  - the number of resource rule validations processed by ACF2/CICS and the number of requests that were aborted (denied) by ACF2/CICS

  - the number of dataset rule validations performed by ACF2/CICS. Note, standard ACF2/CICS does not perform dataset access validations. CICS application programs can request this validation through ACF2/CICS. SG keeps track of these requests.

* SK - displays information about the ACF2/CICS subtask including:

  - the number of times the subtask was inactive because no work was waiting to be processed

  - the number of requests processed by the ACF2/CICS subtask

  - the number of queuing contentions detected. Applies only to multi-processing environments where multiple CPUs process tasks in a single address space.

PRIORITY	CICSPRI	
RSL	CICSRSL	
TRANSEC	CICSKEY	- contains first three bytes of the security key
	CICSKEYX	- contains last five bytes of the security key

1. The ACF2 Logonid (LID) must be 1-8 characters in length with no imbedded blanks. CICS operator-ids (OPIDs) can be 1-20 characters in length and can contain blanks. ACFAESTC uses the first 8 non-blank characters found in the SNT NAME field to form the ACF2 Logonid (LID).

2. An ACF2 password must be 1-8 characters in length with no imbedded blanks. The CICS password is also 1-8 characters in length but can contain blanks.

   If the CICS password does not contain any blanks, it is copied as the ACF2 Logonid password.

   If the CICS password contains a blank, ACFAESTC uses "NEWPASS" as the ACF2 password. For example, a CICS password of "ABC DEFG" becomes an ACF2 password of "NEWPASS".

3. The ACF2 NAME field contains the full name from the SNT NAME field.

ACFAESTC Input Parameters

ACFAESTC requires only one input parameter, MODEL=llllllll; where llllllll names an existing ACF2 Logonid record to be used as a prototype.

For example, this MODEL might contain the following ACF2 Logonid record fields/values to be copied into every new ACF2 Logonid record:

    CICS MAXDAYS(30) MINDAYS(1) IDLE(5)

The installation might also want to include unique Logonid records fields such as values for the fields that form the ACF2 User Identification String (UID).

If no MODEL=llllllll parameter is specified, the default is MODEL=CICSMODL.

SUMMARY OF ACF2/CICS PARAMETER OPTIONS

The following is a summary of the ACF2/CICS parameter options:

	Parameter	Function
	ABCODE	Identify the 3-character abend code prefix.
*	ACFM	Provide security controls for master terminal functions.
	ACMCBEXT	Establish number of user bytes in the ACMCB.
*	CICSKEY	Establish security controls over CICS system resources.
	DCON	Specify terminal disconnect options during violations.
*	DEFAULT	Identify default Logonid information.
	EXIT	Identify the name of the installation's CICS exit program.
	EXITxxxx	Indicate whether an exit is enabled or disabled.
	GMTEXT	Provide from 1 to 55 bytes of "good morning" text.
	LOGON	Sign on a terminal during initialization.
	MAXVIO	Establish a maximum violation threshold for a CICS system.
	MODE	Specify the security mode for ACF2/CICS.
	OPTION	Establish specialized control options.
*	SIGNON	Specify signon control options for a CICS system.
*	SOURCE	Control format of source information during rule interpret.
*	SUBTASK	Establish OS subtask control.
*	SUSPEND	Provide control over when a user is suspended.
	TMA	Establish a Terminal Management Area for a CICS system.
	TRACEID	Declare a CICS user traceid for ACF2/CICS.
*	UCA	Establish User Control Area controls.
*	USERKEY	Establish security controls over user resources.
	VALCONS	Indicate whether system console transactions are validated.
*	VERIFY	Specify password re-verification facility control.
	WTO	Write a message to system console during initialization.
	WTOIxxx	Control informational console messages.
	WTOSxxx	Control security console messages.
	WTOVxxx	Control violation console messages.

- TCT=YES/NO - specifies whether ACF2/CICS will update the terminal operator fields in the TCTTE with the values contained in the user's Logonid record. This is a new subparameter in Release 4.1.

- TRANOFF=CSSF/tttt - identifies the sign-off transaction code. Replaces the CSSF parameter of Release 4.0.

- TRANON=CSSN/tttt - identifies the signon transaction code. Replaces the CSSN parameter of Release 4.0.

- TCTTEXSA=YES/NO - specifies whether the address of a local copy of the terminal's ACMCB will be placed in field TCTTEXSA in the terminal's TCTTE. This new Release 4.1 subparameter supersedes the ANCHOR=TCTTE parameter of Release 4.0. Note also that the TCTTEXSA=YES allows the installation to examine a local copy of the terminals ACMCB. The installation cannot directly modify the real ACMCB address as was permitted under Release 4.0. TCTTEXSA is provided only as a compatibility aid for sites requiring access to an ACMCB. SKK recommends all installation-written exit programs that require information contained in the ACMCB be modified to use the "Usercall" facility of ACF2/CICS.

* SOURCE=TCT/VTAM - specifies the method used to construct source names. When SOURCE=TCT, the source name is set to the value of field TCTTETI in the terminal's TCTTE. When SOURCE=VTAM, the source name is set as it appears in the node information block within the terminal's TCTTE. This is a new parameter in Release 4.1.

* SUBTASK=LOGON/NO - specifies subtasking options for Release 4.1. The RULE option is no longer available in Release 4.1.

* SUSPEND - is a new parameter in Release 4.1. It includes two subparameters:

  - PASSWORD=YES/NO - specifies whether a user's Logonid is to be suspended when the maximum number of allowed invalid password violations is reached. This subparameter supersedes the SUSPSWD parameter of Release 4.0.

  - VIOLATION=YES/NO - specifies whether a user's Logonid is to be suspended when the maximum number of allowed violations is reached. This subparameter supersedes the SUSVIOL parameter of Release 4.0.

* UCA POOL=nnn,SIZE=nnn - specifies the number and size (in bytes) of User Control Areas (UCAs) that ACF2/CICS will allocate for its use. The default is "UCA POOL=80,SIZE=1500". By properly using the UCA pool, the installation can ensure that ACF2/CICS operates efficiently. This parameter supersedes the SLOT and CACHE parameters of Release 4.0.

If your installation uses CICS Release 1 Version 5, an appropriate ACF2/CICS security subsystem is available. Contact your local ACF2 Technical Support Representative to obtain documentation for this support.

In anticipation of these future uses of SAF, the following improvements are incorporated into the Release 4.1 level of the ACF2/SAF interface:

* The ACF2/SAF interface is installed as part of the Release 4.1 base product via SMP. A new operand, called SAF, has been added to the OPTS global system options record. Specify SAF to activate the interface. The default is NOSAF.

* Default values are recommended for the SAFSAFE global system options record. Use of these defaults eliminates potential duplicate access validations. A sample jobstream, called SAFSAFE, is provided on the Release 4.1 distribution tape to automatically insert the recommended GSO SAFSAFE records into the ACF2 Infostorage Database.

* A new GSO record called SAFMAP is provided. SAFMAP allows the installation to define a unique ACF2 generalized resource type for each SAF-defined resource class. IBM continues to define new resource classes and SAF implementations. SKK anticipates that the SAFMAP records can be used to quickly and easily accommodate all new resource classes and provide flexible ACF2 generalized resource control for the related resources.

<u>SAF/NOSAF Global System Option</u>

The Release 4.1 ACF2/SAF interface is automatically installed with standard acf2/MVS via SMP. In Release 4.0, a separate link-edit was required to activate the ACF2/SAF interface.

A new SAF/NOSAF option is added to the OPTS global system options record to control the ACF2/SAF interface. Specify SAF to activate the ACF2/SAF interface or NOSAF to deactivate the interface. The default is NOSAF.

APPL (Applications)
GLOBAL (for Global Access Checking)
GMBR (for Global Access Checking)

Basically, a SAFMAPS record associates an IBM-defined or other vendor-defined SAF resource class to an ACF2 generalized resource type. ACF2 can then validate access to the resource using standard generalized resource rules.

A SAFMAP record has the following format:

    SAFMAPS MAPS(type1/class1,...typen/classn)

Up to 128 different types and classes can be defined.

For example, if a SAF resource class is defined as TCICSTRN and you want to associate it to an ACF2 generalized resource type of CKC, the following SAFMAPS record is required:

    SAFMAPS MAPS(CKC/TCICSTRN)

Note that masking can be used to specify the SAF "class". For example, to associate the SAF classes TCICSTRN and GCICSTRN to the ACF2 resource type of CKC, the following SAFMAPS record is required:

    SAFMAPS MAPS(CKC/*CICSTRN)

The default SAFMAPS record is:

    SAFMAPS MAPS(SAF/-)

The default causes all SAF classes to be associated with a resource type of SAF.

The SAFMAPS record can be activated dynamically by executing an "F ACF2,REFRESH(SAFMAPS)" command from the system operator's console.

TS778114 - PROGRAM PATHING IMPROVEMENTS

Release 4.1 can more accurately determine the name of the library from which a program is loaded for execution. This includes instances where multiple libraries are concatenated in a JOBLIB or STEPLIB statement. This enhancement eliminates the UNKNOWN.LIBRARY condition during program pathing validation that sometimes occurred in previous releases.

How ACF2 Validates Access When Libraries Are Concatenated

ACF2 also recognizes concatenations. When found (either JOBLIB or STEPLIB), access validation for each library in the concatenation is performed. For example:

```
//PAYPROD  JOB ............
//JOBLIB   DD DSN=PAYROLL.PROD.LOAD,DISP=SHR
//         DD DSN=PAYROLL.TEST.LOAD,DISP=SHR
//MSTREAD  EXEC PGM=PRODMST
//MSTFILE  DD DSN=PAYROLL.PROD.MASTER,DISP=SHR
...
```

Assuming the above JCL is being used, ACF2 will validate, according to standard ACF2 access rules and user privileges, that the Logonid of the user who submitted the job is authorized for execute access to all the libraries in the concatenation (PAYROLL.PROD.LOAD and PAYROLL.TEST.LOAD in the example). Validation of execute access to these two libraries is done before the program (PRODMST in the example) is actually loaded for execution.

Using the GSO LINKLST Record to Consolidate Rules

Under 4.1, ACF2 retains the name of the library from which a program was loaded for execution, even if it came from a system linklist library. Therefore, an UNKNOWN.LIBRARY condition will never occur. This means program pathed access rules can always explicitly define the library from which the program must be loaded.

To simplify rule writing and ensure compatibility between Releases 4.1 and 4.0, ACF2 will substitute LIB('SYS1.LINKLIB') <u>only</u> when the program being executed is loaded from a library defined in the LINKLST global system options record.

Therefore, all libraries that are to be equated to SYS1.LINKLIB for rule validation purposes must be defined in the LINKLST record. Libraries defined as part of the system linklist (via SYS1.PARMLIB) <u>must</u> also be defined in the LINKLST record if compatibility with existing 4.0 program pathing rules is desired.

TS72943 - DYNAMICALLY ALLOCATE SEQUENTIAL BACKUP DATABASES

Release 4.1 dynamically allocates the sequential backup datasets for the ACF2 databases. Thus installations can now process their sequential backup datasets while ACF2 is running.

Under 4.1, acf2/MVS allocates the sequential backup databases specified in the global system options BACKUP record at initialization time and then immediately deallocates them so the installation can use them if required. When automatic backup processing begins, the sequential backups are dynamically allocated for use and then deallocated after backup processing completes.

If acf2/MVS is unable to dynamically allocate a sequential backup database when required (e.g., during acf2/MVS initialization or during automatic backup processing), a warning message is issued to the console operator to inform him of the failure and other acf2/MVS processing continues.

Release 4.1 also adds a new WORKUNIT operand to the BACKUP record. WORKUNIT defines the type of device on which ACF2 will dynamically allocate work files during automatic backup of the ACF2 databases.

Definition of WORKUNIT allows ACF2 to dynamically allocate backup work files when automatic backup processing begins. This ensures that disk cleanup programs do not scratch work files while ACF2 is running, which could destabilize ACF2.

The default is WORKUNIT(VIO) or virtual input/output device. The installation can choose any device type desired. ACF2 dynamically calculates the amount of work space needed and allocates the space.

If ACF2 is unable to dynamically allocate the required space during backup processing, a message is sent to the system operator highlighting the condition. Other ACF2 processing continues normally. Similarly, if the WORKUNIT operand is not specified, an informational message is sent to the system operator and other ACF2 processing continues normally.

TS76071 - ACF2/MVS RELEASE NUMBER ADDED TO ACF2 SMF RECORD

The System Management Facility (SMF) record generated by acf2/MVS now includes the product release level. Installations that use their own reporting routines can make use of the release level if desired.

RELEASE 4.1 MAINTENANCE UPDATES

The following list of maintenance related STAR (Symptom Tracking and Reporting) numbers are included in acf2/MVS Release 4.1:

TS72346	TS74331	TS74441	TS74975	TS76580	TS78028
TS72580	TS74333	TS74443	TS74977	TS76584	TS78068
TS72586	TS74340	TS74444	TS74978	TS76588	TS78071
TS72599	TS74342	TS74445	TS74983	TS76589	TS78081
TS72963	TS74343	TS74446	TS74988	TS76591	TS78085
TS73188	TS74345	TS74447	TS74989	TS76592	TS78088
TS73189	TS74348	TS74448	TS74990	TS76593	TS78089
TS73190	TS74350	TS74583	TS74997	TS76597	TS78091
TS73629	TS74353	TS74592	TS74998	TS76688	TS78109
TS73664	TS74354	TS74593	TS74999	TS76689	TS78119
TS73722	TS74357	TS74597	TS75128	TS76800	TS78401
TS73777	TS74364	TS74620	TS75260	TS76855	TS78450
TS73778	TS74380	TS74660	TS75262	TS76858	TS78463
TS73781	TS74389	TS74666	TS75263	TS76874	TS78530
TS73782	TS74391	TS74670	TS75272	TS76884	TS78531
TS73783	TS74393	TS74683	TS75273	TS76887	TS78532
TS73788	TS74396	TS74687	TS75277	TS76888	TS78534
TS73789	TS74398	TS74688	TS75303	TS77188	TS78535
TS73957	TS74399	TS74689	TS75384	TS77332	TS78537
TS74079	TS74401	TS74753	TS75385	TS77336	TS78538
TS74080	TS74402	TS74755	TS75388	TS77542	TS78539
TS74096	TS74403	TS74805	TS75762	TS77618	TS78540
TS74205	TS74405	TS74812	TS75777	TS77653	TS78541
TS74210	TS74406	TS74819	TS75780	TS77661	TS78542
TS74211	TS74407	TS74820	TS75787	TS77674	TS78543
TS74215	TS74408	TS74822	TS75788	TS77675	TS78544
TS74219	TS74409	TS74823	TS75793	TS77676	TS78545
TS74221	TS74410	TS74824	TS75797	TS77681	TS78547
TS74228	TS74411	TS74825	TS75997	TS77683	TS78549
TS74231	TS74412	TS74826	TS76059	TS77684	TS78550
TS74303	TS74413	TS74830	TS76063	TS77686	TS78551
TS74307	TS74414	TS74832	TS76069	TS77688	TS78552
TS74310	TS74416	TS74835	TS76075	TS77691	TS78553
TS74312	TS74417	TS74927	TS76093	TS77692	TS78554
TS74314	TS74418	TS74929	TS76116	TS77693	TS78555
TS74316	TS74419	TS74933	TS76122	TS77694	TS78556
TS74318	TS74422	TS74943	TS76123	TS77695	TS78557
TS74319	TS74423	TS74953	TS76135	TS77697	TS78558
TS74322	TS74424	TS74955	TS76353	TS77699	TS78559
TS74324	TS74425	TS74959	TS76554	TS77793	TS78560
TS74325	TS74426	TS74963	TS76569	TS77928	TS78561
TS74327	TS74427	TS74966	TS76570	TS77929	TS78562
TS74328	TS74430	TS74968	TS76571	TS77936	TS78563
TS74329	TS74431	TS74972	TS76573	TS77938	TS78564
TS74330	TS74440	TS74973	TS76574	TS78025	TS78565

Systems Software and Consulting

SKK, Inc. 10400 West Higgins Road Rosemont, IL 60018 (312) 635-1040

Product Support (312) 635-3000 Telex 206 186 SKK ROSM

January 31, 1986

TECHNICAL NEWSLETTER

Publication:	ACF2 Change Summary
Publication Number:	AMG4039-01
Release:	4.1 (MVS)
Dated:	January 31, 1986

Previous Publication Name:	ACF2 Change Summary
Publication Number:	AMG4039-00
Release:	4.0 (MVS)
Dated:	January 15, 1985

This technical newsletter is part of the ACF2 system and provides updated information for the specified publication. This TNL is a total replacement of this manual. Please replace your previous copy of this manual with the enclosed new copy dated January 31, 1986.

Changes and additions since the last release of this manual are shown by the presence of a change bar (|) in the left margin of the page.

Note: Please file this cover letter at the back of the base publication to provide a record of changes.

acf2™

The Access Control Facility

ENHANCEMENT SUMMARY

for

acf2/MVS Release 4.0

Base Document Dated: December 10, 1984

Doc. Nr. AMG4039-00

Printed in U.S.A.

ACF2 is a proprietary product developed and maintained by:

SKK, Inc.
10400 West Higgins Road
Rosemont, Illinois 60018-9990

Business Office: (312) 635-1040
Product Support: (312) 635-3000
TELEX: 206-186 (SKK ROSM)

A 24 hour answering service on (312) 825-5150 is available
for emergency assistance outside of normal business hours.

TABLE OF CONTENTS

SUMMARY OF ENHANCEMENTS

acf2/MVS Release 4.0 includes many new enhancements that benefit security administrators, auditors, system maintenance personnel, and system users. The major enhancements are listed below, grouped by functional category. Additional information about each enhancement is included elsewhere in this document as indicated by the page number references.

MORE FLEXIBILITY AND CONTROL FOR SECURITY ADMINISTRATORS

Many of the acf2/MVS Release 4.0 enhancements give security administrators increased capability to easily control the acf2/MVS system, such as:

* Complete authority over all ACF2 global system options. This major enhancement allows security administrators to store ACF2 control options on the Infostorage Database and then dynamically activate options without relying on maintenance personnel to reassemble macros or IPL the system. See TS77555, page 5.

* A new MAINT Logonid record privilege that provides more effective control of users and programs that perform system maintenance functions (such as disk backup, restore, etc.). This also allows the security administrator to better differentiate this function from other privileges and provides more specific controls.

  See TS79135, page 9.

* A new method to discretely monitor and record a user's system accesses to provide better security in especially sensitive areas. See TS78019, page 10.

* An optional automatic data erase feature that physically erases disk files when they are deleted. For example, this feature eliminates the possibility of someone reading residual data from uncataloged datasets. In addition, this facility also supports the the U.S. Department od Defense "object release" data protection requirements. See NOTE #7, page 10.

* A new option to control control operator initiation of Started Tasks (STCs) using ACF2 time/shift records. See TS79152, page 12.

* Option to grant a user read-only access authority to the ACF2 Infostorage Database. For example, this will allow scoped security or account users to display (but not alter) their scope list record. See TS79152, page 12.

* A new SHOW ACF subcommand that displays all the ACF2 system options at one time in response to one command. See TS72702, page 12.

* An option to write all secured volume access rules in one rule set, which reduces the number of rule sets the administrator must maintain. See TS73494, page 13.

* Ability to more easily control Build Generation Data Group (BLDG) requests using a single ACF2 rule entry. See TS73480, page 13.

NEW ACF2 REPORTING AND AUDITING FEATURES

Many new ACF2 reporting and auditing features are incorporated in acf2/MVS Release 4.0. Major enhancements include:

* A new Environment Report (ACFRPTNV) that provides a complete audit trail of system activities, such as IPLs, shutdowns, changes to the ACF2 security environment, loss of System Management Facility (SMF) data, etc. Using the ACFRPTNV report, administrators and auditors can determine what changes were made to the security environment and by whom, as well as detecting possible loses of SMF data or other security related operational problems. See TS73836, page 14.

* The Information Storage Update Log (ACFRPTEL) now prints before and after values of modified global system option record fields. This gives administrators and auditors a clear picture of what specific records and options were changed, when, and by whom. See TS79277, page 15.

* The Logonid Modification Log (ACFRPTLL) now also prints before and after values of individual modified Logonid record fields so that administrators and auditors can easily identify changes in a user's security level. See TS73994, page 15.

* Many ACF2 SMF records now contain additional data and all have been combined under a single record type which simplifies auditing of ACF2-controlled systems, local report generator processing, etc. See TS73453, page 17.

* ACF2 Pre-Processor Utility (ACFRPTPP) shows the creation date and time of the first and last SMF records processed so that auditors and administrators can more easily determine if all SMF data has been properly included in their reports. See TS77438, page 18.

TSO ENHANCEMENTS

For sites that use IBM's Time Sharing Option (TSO or TSO/E), acf2/MVS Release 4.0 provides the following new features and enhancements:

* Fullscreen logon support for all TSO and TSO/E releases which simplifies user logon procedures. (Note that TSO/E is not required.) See TS73816, page 20.

* Optional full validation of Operator Identification (OID) Cards at system entry time, providing another means to validate a user's access to the system. See TS77823, page 21.

* Enhanced support flexibility for all device types (ASCII, TWX, 327x, 2741, etc.) is provided to ensure that user passwords are fully protected. See TS75924, page 21.

* Unique local logon keywords can be defined in the ACF2 Infostorage Database, eliminating the need for special modifications to ACF2 and TSO. See TS73944, page 22.

* Full support for the UADS tree structure is provided so that authorized users can easily select the appropriate account numbers, performance groups, and logon procedures at TSO logon time. See TS77580, page 22.

* To avoid the effects of keying errors when entering a new password, ACF2 requires that new passwords be entered twice during logon or sign-on. See TS75952, page 23.

NEW AND ENHANCED INTERFACES FOR OTHER VENDOR SOFTWARE PRODUCTS

acf2/MVS Release 4.0 includes some major new interfaces to help security administrators effectively control the activities of users of other widely used software products. New interfaces include

* A completely new ACF2/CICS security system. ACF2/CICS is a comprehensive security system designed to address all the security needs of today's CICS applications. See TS73685, page 24.

* A direct interface to IBM's System Authorization Facility (SAF) which can provide ACF2 security for all software products that use SAF. See TS72592, page 26.

* An extensive security interface for Cullinet's Integrated Database Management System Data Communications Product (IDMS-DC), Integrated Database Management System (IDMS-DB), and Universal Communications Facility (UCF) products. See TS73914, page 27.

* Added optional validation of PSBs (Program Specification Blocks) in an IMS environment. See NOTE #8, page 28.

* A new usermod for users of the PDSMAN library manager that can provide member level security for partitioned datasets.

ENHANCEMENTS FOR SYSTEMS MAINTENANCE PERSONNEL

acf2/MVS Release 4.0 includes many technical enhancements that help system maintenance personnel efficiently install, maintain, and test ACF2. Technical enhancements include:

* A streamlined installation process that greatly simplifies ACF2 installation and maintenance. See TS73390, page 29.

* ACF2 intercepts are dynamically implanted at ACF2 startup time, eliminating POSTJOBs. See TS73390, page 29.

* The new global systems options (GSO) feature eliminates most of the Field Definition Record Generation (ACFFDR) macros and substantially reduces the amount of time system programmers must devote to ACFFDR maintenance. See TS77555, page 5.

INCREASED CONTROL FOR SECURITY OFFICERS

TS77555 - ACF2 SYSTEM CONTROL OPTIONS CAN BE DYNAMICALLY ACTIVATED

As a major benefit to security administrators and system maintenance personnel, almost all of the ACF2 global system options can now be dynamically changed and activated. Administrators benefit greatly from this feature because they have more control over ACF2 global system options and can dynamically change options as desired.

System maintenance personnel benefit from reduced workload and added flexibility to test the more technically oriented options. Administrators and auditors also benefit because ACF2 keeps a complete audit trail of all changes to global system options including before and after change values and the date and time that options are activated (see TS73836, page 14, and TS79277, page 15).

GSO Records Are Stored on the Infostorage Database

Prior to acf2/MVS Release 4.0, all ACF2 system options were selected by coding a set of macros which comprised the ACF2 Field Definition Record (ACFFDR). Since these options were coded in macros, a reassembly and system IPL was required to activate a change to an ACF2 system option.

With acf2/MVS Release 4.0, security administrators will store ACF2 global system options as records (called GSO records) on the ACF2 Infostorage Database. Each GSO record consists of a record key and a series of operand fields.

The format of a GSO record key is:

CGSO<sysid-mask><recid-mask>

where:

C - is a constant type code representing ACF2 storage class C, which stands for CONTROL.

GSO - is a constant representing global system option (GSO) type control records.

<sysid-mask> - is an installation defined 1-8 character name that can be used to separate GSO records into logical groups per system or CPU.

<recid-mask> - an SKK defined 1-16 character name that identifies the function of the GSO record. These recids correspond closely to the names of the ACFFDR macros used in prior ACF2 releases (e.g., BACKUP, OPTS, RESVOLS, SECVOLS, TSO, etc.).

The operand (or data) area of each GSO record contains the specific option selection and parameter values for each individual GSO record. The exact content varies depending on which recid is specified. For example, the operands define for the BACKUP GSO record are TIME, STRING, and CPUID.

See "Summary of GSO Records" for a complete list of all the available GSO record identifiers (recids).

GSO Records Can Be Grouped by System

Another significant benefit of GSO is that security administrators can easily group GSO records into functional sets. Multi-CPU sites will find this feature particularly beneficial. For example, in a two or three CPU shop, separate sets of GSO records can be created for each CPU with completely different ACF2 options defined for each CPU. Alternatively, the installation may create a single set of common GSO records to be shared by all systems or use the sysid-mask to share specific GSO records between systems.

GSO Records Maintained Via the ACF Command

ACF2 global system options (GSO) records are easily inserted, changed, deleted, and listed using the ACF command in online interactive mode, in batch mode, or through ACF2/SPF panels. This provides security administrators with complete flexibility and control over GSO records.

A new ACF command mode, CONTROL, is provided to manipulate GSO records. The following ACF subcommands are provided for entering CONTROL mode and maintaining GSO records:

SET CONTROL(GSO) - places the ACF command in CONTROL mode

SET SYSID(sysid) - to set the default sysid for this session

SET MSYS(sysid-mask) - to set the default sysid to a mask

INSERT - to create a new GSO record

CHANGE - to modify an existing GSO record

LIST - to display GSO records

DELETE - to remove a GSO record

Optionally, the administrator can use the SET SYSID(sysid) or SET MSYS(sysid-mask) subcommands when manipulating GSO records. SET SYSID is useful when working with a single group of GSO records because it frees the administrator from having to state the sysid on each subcommand line. SET MSYS(sysid) is ideal when working with multiple groups of GSO records (e.g., for changing or listing groups of records).

Operator Commands Dynamically Activate GSO Records

Security administrators can dynamically activate GSO records and monitor GSO activities using five new system operator modify commands (i.e., F ACF2,...). These operator commands allow the security administrator to:

REFRESH(recid/ALL) - immediately activate GSO options. A single record (such as OPTS) can be activated or a completely new group of GSO records can be activated. To use REFRESH, the issuer must have the new REFRESH privilege in his/her Logonid record. When a REFRESH command is entered from the system console, ACF2 prompts the issuer for a Logonid/password and verifies that the issuer is authorized to use REFRESH.

SHOWGSO - displays the current GSO TRACE options (see below).

SHOWSYS - displays the sysid of the active GSO options. Can be used to verify that the correct group of GSO records is active.

SETSYS(sysid) - allows the administrator to easily migrate from one group of GSO records to another. It is generally used prior to the REFRESH command to select the sysid of the GSO records and operands required.

TRACE - gives administrators and systems maintenance personnel the option of displaying GSO activity records on the system console, writing them in the system log, or both. Convenient for special testing situations, auditing, etc.

Security administrators and auditors can readily obtain a complete report on the use of these ACF2 system operator commands. The new ACF2 Environment Report (ACFRPTNV) shows each modify command issued, the parameters selected, the date and time the command was issued, and the console used (see TS73836, page 14).

Program Provided to Convert ACFFDR into GSO Records

Administrators can easily convert their current ACFFDR into GSO records using a new utility program called GSOAID. GSOAID accepts the ACFFDR load module as input and automatically creates a sequential dataset in IDCAMS format. The IDCAMS utility can then be used to insert the resultant GSO records into the ACF2 Infostorage Database. The process should take no more than 10 minutes to complete. GSOAID will process acf2/MVS Release 3.1.3 3.1.4, or 3.1.5 ACFFDR modules.

Summary of GSO Records

With acf2/MVS Release 4.0, the following global system option (GSO) records are stored on the ACF2 Infostorage Database. Note that in prior acf2/MVS releases, all of these GSO records were defined via ACF2 Field Definition Record Generation (ACFFDR) macros but have been removed from the Release 4.0 ACFFDR.

BACKUP - selects options for automatic backup of the three ACF2 VSAM databases.

BLPPGM - defines the programs that are authorized to use Bypass Label Processing (BLP) for tape files.

EXITS - contains the module names of all installation-written exits.

LINKLIST - allows selected libraries to be treated as part of the system's logical linklist (SYS1.LINKLIB). library.

LOGPGM - defines the set of executable programs for which ACF2 will write an SMF logging record for every dataset access request.

MAINT - defines programs that are used for system maintenance purposes (e.g., archival, backup, disk compression, etc.) and the users authorized to use them on all datasets/volumes without ACF2 rule validation or logging.

NJE - selects the Network Job Entry options in ACF2-controlled JES2 and JES3 environments.

OPTS - selects various global control options for the ACF2 system. For example, ACF2 security mode, the default Logonid for batch jobs, maximum number of security violations allowed in a single session or batch job, etc.

PPGM - defines the set of protected programs.

PSWD - selects the ACF2 password options.

RESDIR - specifies the resource rule sets for which an instorage directory will be built and maintained by ACF2.

RESRULE - defines the access rule sets that are to be made resident in the system Common Storage Area (CSA).

RESVOLS - selects the set of volumes that ACF2 will protect at the dataset name level.

SECVOLS - defines the set of volumes that ACF2 will protect at the volume level.

TSO - specifies the ACF2 options related to TSO sessions.

WARN - selects message text that is displayed when the ACF2 system is in WARN mode.

A number of options related to TSO support are also defined via GSO records. Note that these new GSO records replace certain tables (CSECTs) used by prior ACF2 releases.

TSOCRT - selects a clear string for ASCII CRT devices so that the ACF2 password field is immediately cleared from ASCII CRT devices. Replaces the ACF$CRT CSECT. See TS75924, page 21.

TSOKEYS - specifies installation dependent TSO logon keywords. Replaces the ACF$KEYS CSECT. See TS73944, page 22.

TSOTWX - defines a control sequence that will be sent to TWX-type devices to mask the ACF2 password during logon/sign-on processing. Replaces the ACF$TWX CSECT. See TS75924, page 21.

TSO2741 - selects a mask string which is sent to IBM 274x terminals during logon/sign-on processing to obscure the user's password. Replaces the ACF$2741 CSECT. See TS75924, page 21.

Summary of Macros That Remain in the ACFFDR

The following ACF2 Field Definition Record (ACFFDR) macros remain active for acf2/MVS Release 4.0.

@CFDE @CSVC @DDSN @GENFDR @GROUP @HEADER @MLID

@MUSASS @SETUP @SMF @UID @ZEROFLD

As in prior acf2/MVS systems, Release 4.0 requires that the installation generate an ACFFDR module using these macros. A reassembly and IPL is required to activate changes made to the ACFFDR macros.

TS79135 - MAINT PRIVILEGE CONTROLS MAINTENANCE PROGRAMS

Security administrators have been provided with another option for controlling Logonids that are used for system maintenance processing. To activate this new feature, the security administrator simply assigns the new MAINT attribute to Logonid records that are used to perform system maintenance functions (e.g., disk backup, file restores, etc.) and defines the related Logonid, library, and program name combination in a MAINT global system options (GSO) record.

Prior to acf2/MVS Release 4.0, the security administrator had to define a maintenance Logonid with the NON-CNCL (non-cancellable) attribute as well as inserting the Logonid, library, and program name in an @MAINT macro in the ACFFDR.

Under Release 4.0, ACF2 will search the MAINT global system options (GSO) record for a match whenever a Logonid with MAINT or NON-CNCL makes its initial dataset access request. If a match is found, all subsequent rule validation is bypassed.

A major benefit of using MAINT is that the maintenance Logonid need not be given the NON-CNCL attribute, minimizing the possibility of using a NON-CNCL Logonid for unauthorized use.

TS78019 - NEW USER MONITORING AND LOGGING FACILITY

A new method for monitoring and logging (MON-LOG) a user's system accesses is provided in acf2/MVS Release 4.0. Using MON-LOG, security administrators and auditors can discretely monitor a user's system accesses. One major benefit of MON-LOG is that system operators are not informed when a monitored user accesses the system (i.e., no console message is generated).

To activate the monitor and logging feature, the administrator uses the ACF command to turn on the MON-LOG bit field in the desired user's Logonid record. Whenever the monitored user accesses the system (e.g., TSO logon, CICS sign-on, etc.), ACF2 writes an SMF record detailing the date, time, CPU, and input device of the system access. These SMF records are processed by the ACF2 Invalid Password/Authority Log (ACFRPTPW).

NOTE#7 - AUTOMATIC DATA ERASE FACILITY DESTROYS RESIDUAL DATA

Sites concerned about the possibility that residual data from deleted datasets can be retrieved and reviewed by unauthorized personnel will benefit from the Automatic Data Erase Facility provided in acf2/MVS Release 4.0. Installation and use of the data erase facility is completely optional and is distributed as SKK NOTE #7.

When the automatic erase facility is used, ACF2 physically erases all data residing in a direct access storage dataset when the dataset is deleted. Physical erasure takes place before the disk space is returned to the system for later reallocation. The following chart illustrates the different types of data versus various protection mechanisms:

PROTECTION MECHANISMS

DATA TYPE	JCL	SVC99	Utilities	NOTE #7
Permanent VSAM	I	I	U	S
Permanent Non-VSAM	I	I	U(ACF2)	S
Temporary Non-VSAM Non-VIO	I	I	U(ACF2)	S
Temporary Non-VSAM VIO	S	S	S	S

where:

I = impossible
U = user action required
U(ACF2) = possible with user-invoked ACF2 utilities
S = action automatically taken by system

The NOTE #7 technique is provided in two parts: VSAM and non-VSAM. The non-VSAM feature is invoked via JCL, dynamic unallocation (SVC99), system utilities (IEHPROGM, IDCAMS), or a user program. The VSAM feature is invoked during IDCAMS delete processing. Both features are implemented at system-provided exit points and function in both batch and online environments.

Implementation of ACF2 with the NOTE #7 automatic erase feature also provides the added benefit of upgrading an installation to the class C2 level security environment outlined by the U.S. Department of Defense guidelines. For additional information about the class C2 security level, reference Department of Defense Trusted Computer System Evaluation Criteria, Fort George G. Meade, Maryland: Department of Defense Computer Security Center publication CSC-STD-001-83, 15 August 1983.

TS79152 - TIME/SHIFT CONTROLS AVAILABLE FOR STARTED TASKS

Security administrators can now use ACF2 time/shift restrictions to increase their level of control over the use of Started Tasks (STCs).

To place time/shift controls on an STC, the administrator simply includes a SHIFT(shift-name) entry in the desired Logonid record (where shift-name can be the name of a new or existing Infostorage shift record). This shift record defines the valid days, dates, and time periods during which that STC Logonid can be used.

TS77649 - INFORMATION STORAGE READ-ONLY PRIVILEGE AVAILABLE

Security administrators can now grant users permission to display records stored on the ACF2 Infostorage database. This will permit users to display Infostorage records without also granting them authority to change the records.

This new option is called INFOLIST. The security administrator designates which types of users are allowed to display Infostorage records via the INFOLIST field of the OPTS global system option (GSO) record. By default, INFOLIST(SECURITY,AUDIT) is assumed, which allows users with the ACF2 privileges of SECURITY or AUDIT to display all Infostorage records.

Note that generalized resource rules (Infostorage class 'R' records) are still controlled by the DECOMP and %CHANGE options. INFOLIST users will not be allowed to automatically display generalized resource rules unless they have the appropriate DECOMP or %CHANGE authority.

The major benefit of INFOLIST is that privileged users (such as those with the SECURITY or ACCOUNT privilege) can remain scoped, restricting their ability to change certain Infostorage records, while still being permitted to display all records. For example, scoped security officers can be allowed to display Infostorage records, including their scopelist, but not permitted to change any specific records outside their scope.

TS72702 - "SHOW ACF2" SUBCOMMAND DISPLAYS ALL SYSTEM OPTIONS

Security administrators, auditors, and account managers can display all active ACF2 system options via a single request by using the new "SHOW ACF2" subcommand of the ACF2 command. SHOW ACF2 displays all the ACF2 options, both global system options (GSO) and ACFFDR options, and eliminates the need for users to enter multiple SHOW subcommands.

TS73480 - BLDG REQUESTS VALIDATED USING A SINGLE RULE ENTRY

acf2/MVS Release 4.0 can validate Build Generation Data Group (BLDG) requests using a single access rule entry. Security administrators will benefit from this more efficient method of validating BLDG requests because fewer rule entries are required.

For example, a request to build a Generation Data Group (GDG) such as:

```
BLDG INDEX=A.B.C.D,ENTRIES=nn,CVOL=volser
```

can be validated using the follwing one line rule entry:

```
$KEY(A)
 B.C.D UID(PROGRAMMER) ALLOC(x)
```

where x is ALLOW, LOG, or PREVENT

Under prior acf2/MVS releases, four rule sets (one for each index level) or a more global rule (e.g., "dash" rule) were required to grant a user permission to build a GDG.

TS73494 - VOLRULE OPTION PROVIDES FLEXIBILITY FOR VOLUME RULES

Optionally, security administrators can now store all secured volume access rules in one rule set and substantially reduce the number of volume rules.

Prior to acf2/MVS Release 4.0, ACF2 would automatically create a pseudo dataset name of @volser.VOLUME (where "volser" is the DASD/TAPE volume serial number) and validate accesses to secured volumes based on the appropriate @volser.VOLUME rule set.

With Release 4.0, a new VOLRULE/NOVOLRULE field has been added to the OPTS global system options (GSO) record. VOLRULE allows the installation to use the VOLUME.@volser format when access to a secured volume is validated. This option has the benefit of allowing all secured volume access rules to be stored in one rule set under the same high-level index for all secured volume rules.

NOVOLRULE allows the installation to continue using @volser.VOLUME as the pseudo dataset name format for volume access rules. NOVOLRULE is the default.

NEW REPORTING AND AUDITING FEATURES

Many enhancements have been made to the acf2/MVS Release 4.0 report generators. These enhancements are of two main types: enhancements to accommodate other new Release 4.0 features, and enhancements to improve the overall reporting capabilities of the ACF2 system. Where appropriate, page number references are made to the descriptions of other related new Release 4.0 features.

TS73836 - ENVIRONMENT REPORT DETAILS SYSTEM ACTIVITIES

A new ACF2 report, the Environment Report (ACFRPTNV), is available under acf2/MVS Release 4.0. The ACF2 Environment report alerts administrators and auditors to:

* The possibility that the system might have been operational without ACF2 security.

* Any environmental changes to ACF2, such as activation of updated global system option (GSO) records.

* All operator communication with ACF2 via the modify command (i.e., F ACF2,...). This includes the operator's request, the ACF2 responses, and the command completion status.

* Situations where System Management Facility (SMF) data could have been lost.

Using the Environment Report, administrators and auditors have the ability to monitor all operational aspects of their security systems and can ensure that security is always active. Other information contained in the ACF2 Environment Report includes:

* Date and time ACF2 is started (S ACF2) and stopped (P ACF2), including the CPU effected and the console used to enter the start or stop command.

* All occurrances of any environmental change to the ACF2 system made via the ACF2 modify operator command (F ACF2,...). Modify command parameters are shown on the report along with the date, time, and console used to enter the command.

Another benefit provided by ACFRPTNV is the ability to utilize backup copies of SMF files to create a complete ACF2 environment report for an extended period. Input to ACFRPTNV can consist of SMF data from any of the SYS1.MANx datasets, pre-formatted files prepared by the ACF2 Pre-Processor Utility (ACFRPTPP), or backup SMF files, in any combination desired.

The ACF2/SPF report generator facility has also been updated to provide online capability for the Environment Report.

TS79277 - ACFRPTEL PRINTS BEFORE/AFTER VALUES OF INFOSTORAGE GSO RECORDS

The ACF2 Infostorage Update Log (ACFRPTEL) has been enhanced to accommodate the new global system options (GSO) feature. ACFRPTEL will print before and after values of all GSO records that are modified via the ACF command. Reporting of these before and after values is optional. To support this enhancement, two new parameters have been added to ACFRPTEL:

SUMMARY/DETAIL - when DETAIL is selected, the before/after values of all class CGSO record fields that were modified are displayed. SUMMARY causes a report identical to the Version 3.1.5 ACFRPTEL report to be printed.

CLASS(x) - allows selection of Infostorage update records based on storage class. For example, the DETAIL and CLASS(C) options can be selected to generate an ACFRPTEL report showing all modifications (in before/after format) for class C GSO records only.

The ACF2/SPF report generator facility has also been updated to accept the SUMMARY/DETAIL and CLASS parameters for ACFRPTEL.

See TS77555, page 5 for more information about the new Global System Option (GSO) feature.

TS73994 - ACFRPTLL SHOWS BEFORE/AFTER VALUES OF MODIFIED LOGONIDS

Security administrators can now efficiently audit all Logonid record changes using the new detailed Logonid Modification Log (ACFRPTLL). This enhanced Release 4.0 version of ACFRPTLL produces a detailed, easy to read report showing the contents of each affected Logonid record field before the change with the corresponding value after the change.

Deleted and inserted Logonid records are also included in the report. For newly inserted Logonid records, ACFRPTLL shows all fields and values assigned to the new Logonid record. In addition, if a model record was used to create the new Logonid record (e.g, INSERT USING option), ACFRPTLL also shows the name of the model record. This helps administrators ensure that new Logonids are given only those privileges and values needed.

Reporting of before and after images is optional. To support this enhancement, a new parameter option, SUMMARY/DETAIL, has been added to ACFRPTLL:

SUMMARY/DETAIL - when DETAIL is selected, before/after values of all modified Logonid record fields are printed. The SUMMARY option can be used to produce a Logonid Modification Log report identical to the one produced by acf2/MVS Version 3.1.5 systems.

The ACF2/SPF report generator facility has also been updated to accept the SUMMARY/DETAIL parameter for ACFRPTLL.

ACFRPTPW INCLUDES ADDITIONAL SYSTEM ACCESS LOGGINGS

Additional information about system accesses is now available to security administrators and auditors to help them monitor security events and take preventive actions. The ACF2 Invalid Password/Authority Log (ACFRPTPW) has been enhanced to report the following types of system access attempts:

* OID card violations - Release 4.0 can validate operator identification (OID) cards at TSO logon time. When a user is denied access because the proper OID card was not provided during logon, ACF2 writes an SMF record for later reporting on the Invalid Password/Authority Log. See TS77823, page 21.

* MON-LOG users - system accesses by users whose Logonid record contains the new MON-LOG indicator are written to SMF for reporting on the Invalid Password/Authority report. See TS78019, page 10.

ACF2 REPORTS CAN BE PRODUCED BASED ON JOB NAME MASK

Security administrators and auditors can now generate ACF2 reports showing all security loggings incurred by batch jobs, TSO sessions, STCs, etc. A new parameter, JOBMASK, causes ACF2 to select and format logging records for one job or a group of jobs. The new JOBMASK parameter is available for the following ACF2 reports:

* ACFRPTDS - Dataset/Program Event Log
* ACFRPTEL - Information Storage Update Log
* ACFRPTIX - Dataset Index Report
* ACFRPTJL - Restricted Logonid Job Log
* ACFRPTLL - Logonid Modification Log
* ACFRPTPW - Invalid Password/Authority Log
* ACFRPTRL - Ruleid Modification Log

The ACF2/SPF report generator facility has also been updated to accept the JOBMASK parameter for these reports.

TS73453 - ACF2 SMF RECORDS COMBINED UNDER A SINGLE RECORD

acf2/MVS Release 4.0 produces a single System Management Facility (SMF) record type for all ACF2 security loggings. This enhancement reduces the number of SMF record types that need to be managed by security administrators, systems maintenance personnel, and auditors.

Combined Records are Compatible with Existing Releases

SKK has always maintained upward compatibility between acf2/MVS releases and Release 4.0 adheres to this standard. SMF records produced under prior acf2/MVS releases are internally compatible with Release 4.0. All SMF records produced by an acf2/MVS Version 3.1.x system can be used as input to the Release 4.0 report generators and the ACF2 database recovery utility (ACFREVCR). No changes to existing ACF2 report generator JCL or recovery procedures are required in order to process the Release 4.0 SMF records. When the Release 4.0 report generators encounter an SMF record produced by a pre-4.0 system, ACF2 internally converts the record into the Release 4.0 format.

New ACFSMF Macro Ensures Upward Compatibility

Current acf2/MVS Version 3.1.5 sites that have written their own reporting facilities can easily upgrade their programs to ensure compatibility with the Release 4.0 combined SMF record. Release 4.0 includes a new macro, ACFSMF, that quickly converts the desired Version 3.1.5 SMF record descriptions into Release 4.0 format. In most instances, a recompile of the program with the new ACFSMF macro included initially upgrades the installation's program, which means that minimal recoding is necessary.

Assigning SMF Record Numbers

By default, acf2/MVS Release 4.0 uses SMF record type 230, but sites can define any SMF record desired. However, SKK recommends that no previously used ACF2 SMF record type be used for the Release 4.0 combined record. In addition, SMF record types that were previously assigned for ACF2 use (e.g., 220-227) should not be reassigned until the installation is certain they are no longer needed for historical ACF2 reporting, recovery purposes, etc.

TS77438 - ACF2 PRE-PROCESSOR UTILITY (ACFRPTPP) ENHANCED

A number of enhancements have been made to the ACF2 Pre-Processor (ACFRPTPP) utility. The Pre-Processor utility accepts System Management Facility (SMF) files as input and then extracts all the SMF records needed by the various ACF2 report generators. During processing, ACFRPTPP creates one staging file for each type of SMF record relating to ACF2.

* To accommodate the new ACF2 Environment Report (ACFRPTNV), the Pre-Processor (ACFRPTPP) utility creates a new separate file (SMFNR) containing the SMF logging records needed to generate the report. ACFRPTPP will also extract IBM type 0 system IPL records and type 7 SMF data lost records for inclusion on the Environment Report. See TS73836, page 14.

* ACFRPTPP accepts both acf2/MVS Release 4.0 combined SMF records and those SMF records created by pre-4.0 systems. This process is entirely automatic and requires no changes to JCL procedures or ACFRPTPP parameters. When a pre-4.0 format SMF record is encountered, ACF2 automatically converts it into Release 4.0 format and places the reformatted record into the appropriate staging file. See TS73453, page 17.

* The "Summary" portion of the ACFRPTPP report now shows the creation date and time of the earliest and latest SMF records processed. For example, if five SMF files combining both 1983 and 1984 records are used, ACFRPTPP will display the date and creation time of the earliest SMF record (such as 83.216, 23.10) and the latest record (such as 84.100, 10.20) processed. This helps security administrators and auditors ensure there is no period during which ACF2 SMF records were omitted from reporting.

REPORTS ALLOW SELECTION OF SMF RECORDS BASED ON SYSTEM-ID

All ACF2 report generators that process System Management Facility (SMF) records, now accept a system identification (SYSID) parameter. Using SYSID, security administrators and auditors can easily produce individual security event reports for each of their ACF2-controlled systems.

The ACF2/SPF report generator facility has also been updated to accept the SYSID parameter for all reports.

REPORTS ALLOW SELECTION OF SMF RECORDS BASED ON TIME-OF-DAY

All ACF2 report generators that process System Management Facility (SMF) records, now accept starting (STIME) and ending (ETIME) time-of-day values. STIME and ETIME supplement the starting date (SDATE) and ending date (EDATE) parameters that were available in all previous acf2/MVS releases. Using STIME, ETIME, SDATE, and EDATE, administrators and auditors can easily generate ACF2 reports detailing security related events for a specific period of time.

The ACF2/SPF report generator facility has also been updated to accept the STIME and ETIME parameters.

TSO ENHANCEMENTS

TS73816 - OPTIONAL FULL SCREEN LOGON FOR TSO USERS

TSO users can now make use of a full screen logon facility provided in acf2/MVS Release 4.0. ACF2's full screen logon facility allows users to easily change logon parameters and also provides optional logon memory support. With logon memory, all logon parameters entered by the user are stored and then automatically inserted into the logon screen for use during subsequent logons.

Other options and features of the ACF2 full screen logon facility include:

* Security administrators have full control of the ACF2 full screen logon facility. A new bit field has been added to the Logonid record (TSOFSCRN) which, when on, allows a user to logon via the full screen logon facility.

* ACF2 automatically inserts default TSO values into the full screen logon menu which reduces the amount of data users need to manually enter. ACF2 obtains these values and options directly from the user's Logonid record.

* ACF2 supports a new NOFSCREEN keyword at TSO logon time. If a user specifies NOFSCREEN at logon time, the full screen logon menu is not displayed. However, the user is still forced to enter a valid Logonid and password in order to access the system.

* Full screen memory support is optional. Security administrators can activate or deactivate memory support using the new FSRETAIN/NOFSRETAIN option of the TSO global system option record. When memory support is active (FSRETAIN), ACF2 automatically inserts a record for each user on the Infostorage Database. Each record contains the user's full screen logon parameters. Creation and maintenance of these records is completely transparent to the user. In addition, these memory records require no maintenance by security administrators.

* The ACF2 supplied full screen logon menu can easily be modified to add a corporate logo. In addition, an input area for installation defined keywords is provided on the logon screen.

Note also that ACF2 full screen logon support is available for both standard TSO and for TSO/E environments.

TS77823 - FULL VALIDATION OF OPERATOR IDENTIFICATION (OID) CARDS

acf2/MVS Release 4.0 provides support for Operator Jentification Card (OID) validation at TSO system entry time. OID card validation serves as an extension to the standard ACF2 Logonid and password controls. All users are still required to enter their ACF2 Logonid and password in order to logon to TSO.

OID character strings are stored on the ACF2 Infostorage database under a new entry record type of the form: EOID<logonid> where logonid is a user's Logonid identifier. A full range of ACF subcommands (i.e., INSERT, DELETE, CHANGE, and LIST) allow easy maintenance of OID entry records. Security officers can insert OID character strings into the Infostorage database by running the desired card through an OID reader or by manually entering the string. OID entry records can contain up to 100 characters and the data is one-way encrypted for storage in a manner similar to ACF2 user passwords to prevent any possible disclosure.

A new OID bit field has been added to the Logonid record. When OID is set in a user's Logonid record, ACF2 will prompt the user to insert their OID card into the card reader at TSO logon time. Denied system access attempts are recorded for inclusion on the ACF2 Invalid Password/Authority Log (ACFRPTPW).

TS75924 - ENHANCED TERMINAL AND DEVICE SUPPORT

acf2/MVS Release 4.0 adds much flexibility in the area of device support, which benefits all sites that use ASCII, TWX, and 2741 devices for TSO. Release 4.0 supports all of these device types and provides flexible, user-friendly facilities to ensure effective password security.

A standard feature of ACF2 password security is that ACF2 always attempts to obscure the password whenever it is entered by the user. On 327x type devices, ACF2 automatically sets the appropriate attribute bytes so the password is not viewable on the screen. For hardcopy terminals, ACF2 automatically attempts to transmit an x-out mask to obscure the password.

Prior to Release 4.0 (depending on the device types in operation), sites that used ASCII or TWX type devices were sometimes required to apply usermods in order to obscure the ACF2 password during TSO logon. acf2/MVS Release 4.0 eliminates the need to apply most usermods. New Release 4.0 features for device support include:

LGNTERM exit - this exit is taken just before ACF2 requests Logonid and password information from a device during logon processing. It is a TSO Pre-Prompt exit that allows the installation to determine the type of device being used so that the appropriate x-out or ASCII control sequences can be transmitted to the terminal to obscure the password. Before the exit is taken, ACF2 attempts to determine what device is being used and passes this information to the exit. The installation exit can then allow ACF2 to continue normally, override the selected device type, or direct ACF2 to send a special control sequence to the device.

TSOCRT - a new global system option (GSO) record in which the installation can store the correct ASCII CRT clear screen sequence. If, during TSO logon, ACF2 determines that the terminal being used is an ASCII device, the TSOCRT string is automatically transmitted to erase the password. (Replaces the ACF$CRT CSECT.)

TSOTWX - a new global system option (GSO) record in which the installation can store an x-out mask for TWX-type devices. If, during TSO logon, ACF2 determines that the terminal being used is a TWX-type device, the TSOTWX string is automatically transmitted to obscure the ACF2 password. (Replaces the ACF$TWX CSECT.)

TSO2741 - a new global system option (GSO) record in which the installation can store an x-out mask for 2741-type hardcopy devices. If, during TSO logon, ACF2 determines that a 2741-type hardcopy device is being used, the TSO2741 string is automatically transmitted to obscure the ACF2 password. (Replaces the ACF$274x CSECT.)

TS73944 - USER DEFINED TSO LOGON KEYWORDS

Sites that have defined their own unique TSO logon keywords can now store these keywords on the ACF2 Infostorage database.

To make use of the new feature, the administrator inserts the installation's keywords into the new TSOKEYS global systems options (GSO) record. At TSO logon time, ACF2 will recognize the keywords and insert them into the standard TSO Logon Work Area (LWA). Note also that the TSOKEYS record replaces the ACF$KEY CSECT that was used in prior releases of acf2/MVS.

TS77580 - SUPPORT FOR UADS TREE STRUCTURE

This enhancement allows installations running in a UADS(YES) environment to continue using the UADS tree structure to select the appropriate logon procedure, account number, performance group, etc.

Two new fields, UADSINDX and LGN-INDX, have been added to the standard ACF2 Logonid record to support the UADS tree structure.

UADSINDX - specifies a 1-8 character string that will be used as the default UADS tree structure index code. ACF2 will insert this character string into the password field in the user's TSO Logon Work Area (LWA) for later use by standard TSO.

LGN-INDX - a bit flag that permits the user to specify an INDEX() parameter at TSO logon time where the value selected becomes the UADS tree structure code. ACF2 will insert this LGN-INDEX value into the password field in the user's LWA.

TS75952 - REVERIFY REQUIRED WHEN ACF2 FORCES A PASSWORD CHANGE

This enhancement requires TSO and CICS users to enter their new password twice during logon/sign-on processing whenever a new password is supplied. This eliminates the possibility of a user making a typographical error when entering a new password and then receiving a subsequent PASSWORD NOT MATCHED message the next time a logon or sign-on is attempted.

ACF2 can force a user to change passwords when MAXDAYS (maximum days between password changes) is reached and/or when a security administrator manually expires (PSWD-EXP) a Logonid record.

TS77172 - ACF2 SVCA ROUTINE PROVIDES TIGHTER PASSWORD SECURITY

acf2/MVS Release 4.0 routines that validate system access and resource access requests (i.e., the ACF2 SVCA routine) clear user passwords as soon as they are entered. This further strengthens ACF2 password security because it ensures that clear-text passwords are never available in the ACF2 parameter lists.

INTERFACES FOR OTHER PRODUCTS

TS73685 - NEW COMPREHENSIVE ACF2/CICS SECURITY SYSTEM

A new ACF2/CICS security system is provided in acf2/MVS Release 4.0 that provides comprehensive security for transactions, programs, files, DL/I calls, transient data, and temporary storage. The features of the new interface include:

* Sign-on security
* Easy installation, with no required source modifications or macros
* Minimal effect on response time
* Menus to dynamically modify system parameters
* Increased auditability through violation reporting and logging facilities
* Ability to automatically disable a terminal after a specified number of security violations
* Greatly enhanced Multiregion Operation and Intersystem Communication (MRO/ISC) support

System, Resource, and Logonid Security

The ACF2/CICS Release 4.0 system provides security on three major levels: at the system level, at the resource level, and at the individual user, or Logonid, level. The result is a comprehensive approach to the problem of CICS security which maintains the traditional ACF2 philosophy of protection by default.

System security with ACF2/CICS includes access validation for programs, transactions, files, DL/I calls, temporary storage, and transient data. System-wide parameters which define ACF2 options and limits can be set either at initialization time or dynamically, using an online menu-driven facility. Sign-on security features require the entry of a unique personal password in a non-displayable area, thus decreasing the chances of inadvertent disclosure.

Resource security makes use of standard acf2/MVS features to restrict access to specific times of the day, weekdays, or dates. Users can be restricted to certain terminals or groups of terminals. For instance, an operator authorized only to enter information from one set of terminals cannot modify information from another department's terminals.

Installations can also define their own resources to be protected by ACF2/CICS, so that access to portions of files or records can be restricted to certain users. In this way, security can be tailored to the special needs of an installation.

Logonid security ensures that the Logonid record associated with each user's unique Logonid provides an accurate security profile of privileges and authority levels. Logonid records can be created, changed, deleted, and listed through an online CICS menu-driven function.

The user's Logonid is validated before that user can access any CICS resources. Password and general security violations are tabulated separately, and the Logonid can optionally be suspended when an installation-defined number of violations has been reached.

Ease of Use

The ACF2/CICS security system features a straightforward installation process. There is no requirement to assemble macros nor any source modifications to be made, which means that the interface can be up and running in a matter of minutes and is generally unaffected by IBM maintenance to CICS.

Non-technical administrators will appreciate the online, menu-driven functions which provide a straightforward method for implementing security quickly. Each function comes with a tutorial which explains available parameters in English, not computerese.

To expedite the creation of large numbers of similar Logonid records, the ACF2/CICS system allows the security officer to use one record as a prototype to generate a number of others. Fields which are different can then be changed on the pertinent records.

Auditability

The ACF2/CICS security system uses batch reports to monitor violation activity. Four basic reports that are available include:

* The Invalid Password/Authority Log identifies rejected system access attempts.

* The Generalized Resource Event Log describes types of resource access requests, the users requesting access, and if access was allowed, allowed and logged, or prevented.

* The Logonid Access Log displays any rule entries which apply to a particular Logonid.

* The Cross-Reference Report shows all users having access to a particular resource.

Real-time system statistics reporting is also provided, allowing authorized personnel to fine-tune ACF2/CICS system parameters while the system is running.

TS72592 - DIRECT INTERFACE WITH THE SYSTEM AUTHORIZATION FACILITY (SAF)

An important benefit provided by acf2/MVS Release 4.0 is a direct interface with IBM's System Authorization Facility (SAF). IBM and other vendors intend to use the SAF interface with their products in the future and, using the ACF2/SAF interface, ACF2 can provide appropriate security for these products.

The SAF facility first directs control to an optional installation-supplied routine, such as the one provided in acf2/MVS Release 4.0. A SAF system service called the MVS router acts as a centralized control over system security processing by providing a common control function for all products using SAF.

The IBM products interact with the SAF MVS router by means of the RACROUTE macro. This macro provides a parameter list that contains user and resource data. SAF gives this information to ACF2 through the SKK supplied installation exit routine ICHRXT00.

ACF2 builds a parameter list from the information provided to this routine, and then performs validation on the following information if it is present: signon, proc, account, OID card, dataset name, volume name, and generalized resource name. After ACF2 has completed its validation processing, it sends a return code to SAF, recommending that processing should either continue or be terminated.

Since ACF2 already protects resources accessed by many products that will use SAF, acf2/MVS Release 4.0 will also feature a SAF SAFELIST that prevents double validation from occurring. ACF2 will not validate these requests when ICHRXT00 is invoked through SAF. The easily constructed SAF SAFELIST ensures that system efficiency is maintained.

The following IBM products currently use the SAF interface: ICKDSF Release 7.0, DF/DSS Release 2.1, MVS/XA DFP Release 1.2, MVS/370 DFP Release 1.1, and DB2. ACF2 will validate accesses by these and all future products that utilize SAF. ACF2 will also continue to protect resources accessed via those products that do not use SAF so that your installation will have the complete security that it needs.

TS73914 - ACF2 SECURITY INTERFACE FOR THE IDMS PRODUCT FAMILY

acf2/MVS Release 4.0 includes a comprehensive security interface for Cullinet's Integrated Database Management System Data Communications Product (IDMS-DC), Integrated Database Management System (IDMS-DB), and Universal Communications Facility (UCF). Some of the major benefits and features of the ACF2/IDMS interface are:

* Security administrators can use ACF2 generalized resource rules to control access to IDMS transactions, IDMS data areas, IDMS subschemas, and IDMS programs.

* Complete ACF2 password and sign-on security is provided allowing administrators to fully control who can sign-on, what days and time-of-day a user can sign-on, the specific terminal(s) from which a user can access IDMS, etc.

* Duplicate Logonid checking is available to ensure that a Logonid is active on only one terminal at any given time.

* ACF2 security for the Universal Communications Facility (UCF) includes Logonid inheritance so that users accessing IDMS resources through TSO, IMS, or CICS are not required to sign-on again.

* Users can be automatically signed-off IDMS after a specified number of security violations. Optionally, their Logonid can be suspended at this time prohibiting the user from accessing the system until a security officer reauthorizes the Logonid.

* Security administrators and auditors receive comprehensive security event reporting via the ACF2 Generalized Resource Log (ACFRPTRV) and the Invalid Password/Authority Log (ACFRPTPW).

* Full maintenance for the ACF2/IDMS interface is provided by SKK, Inc.

Flexibility and efficiency are inherent in the design of the ACF2/IDMS interface. Security administrators can choose to control all IDMS resources or only selected resources. To assist during initial implementation, a transitional LOG mode is provided as well as assignment of a default Logonid. ACF2/IDMS also makes efficient use of CPU resources because all ACF2 security processing is done in a subtask, outside of IDMS.

NOTE#8 - ACF2 SECURITY FOR IMS EXTENDED TO CONTROL PSBS

Sites that use the IMS batch program (DFSRRC00) to execute IMS applications can now control access to Program Specification Blocks (PSBs). Optional code to validate the use of PSBs in the batch environment is included as a standard feature in acf2/MVS Release 4.0 and is distributed as SKK NOTE #8.

When installed, the PSB name specified in the PARM= field on the DFSRRC00 EXEC statement is validated according to a set of TYPE(PSB) ACF2 generalized resource rules. ACF2 PSB validation occurs at job step initiation time (IEFUSI). PSB access requests that ACF2 considers unauthorized are denied and a violation message is issued to the batch joblog. Security violation records are also written to SMF for later reporting on the ACF2 Generalized Resource Event Log (ACFRPTRV).

The sample NOTE #8 code can also be modified locally to validate other PARM= information on the DFSRRC00 EXEC statement.

ACF2/PDSMAN USERMOD PROVIDES MEMBER LEVEL SECURITY

ACF2 sites that use the PDSMAN product can now fully protect their PDSMAN libraries and members using an optional ACF2/PDSMAN Usermod developed by SKK. PDSMAN is a partitioned dataset (PDS) library manager marketed by Goal Systems International, Inc., 5455 N. High Street, Columbus, Ohio 43214-1193.

The ACF2/PDSMAN Usermod uses standard ACF2 generalized resource rules to validate user accesses to PDSMAN libraries and provides member level security for PDSMAN libraries. Major benefits of the ACF2/PDSMAN Usermod include:

* Substantially enhanced security because access to PDSMAN libraries can be controlled at the member level.

* The Usermod easily accommodates all ACF2/PDSMAN environments.

* Actual installation of the Usermod is a simple process because all ACF2 validation is called from PDSMAN provided, defined exit points.

* Installations can easily integrate ACF2 protection for PDSMAN libraries. For example, PDSMAN libraries that contain sensitive information can be under full ACF2 protection while protection for other libraries can be implemented in phases.

TECHNICAL ENHANCEMENTS

TS73390 - ACF2 INTERCEPTS DYNAMICALLY INSTALLED (POSTJOB ELIMINATED)

acf2/MVS Release 4.0 sites are no longer required to run a POSTJOB after a sysgen or IBM maintenance is applied to the operating system. This change is made possible because acf2/MVS Release 4.0 dynamically installs its intercept code when ACF2 is started.

Another benefit of ACF2's dynamic intercepts is that link-edits of certain IBM modules (such as IBM's IEFUSI, IEFUJI, and IEFACTRT system management modules) are no longer required. Instead, ACF2 intercepts for these modules are inserted dynamically, making them transparent to the installation.

Furthermore, system maintenance personnel will benefit from a streamlined install process. With acf2/MVS Release 4.0, all system updates are made using IBM's System Modification Program (SMP). This allows all modifications to be easily tracked and verified by security administrators and auditors as well as system maintenance personnel.

TS79218 - ACF2/SMF DRIVERS AVAILABLE AS A USERMOD

It is also important to note that acf2/MVS Release 4.0 no longer requires SMF exit drivers. Therefore, the SMF drivers supplied in acf2/MVS Version 3.1.5 (SMFJINT, SMFSINT, and SMFTERM) are not used by Release 4.0. However, because many users have implemented their own SMF modules in the Version 3.1.5 drivers, SKK is making the new, functionally superior, drivers available as an optional ACF2 Usermod. Sites that use the drivers for their own purposes can continue doing so.

TS73470 - BLDVRP MACRO RETURN CODES DISPLAYED BY ACF2 MESSAGE

As a diagnostic aid for sites that use Global Resource Serialization (GRS), the ACF8A002 message now displays the return code issued by IBM's BLDVRP macro.

TS73750 - ACF COMMAND MADE MORE EFFICIENT

Changes have been made to the LIST LIKE(mask) option of the ACF command. These changes are basically performance improvements that substantially reduce I/O requirements when a LIST LIKE(mask) subcommand is executed.