

Department of Veterans Affairs
Decentralized Hospital Computer Program

KERNEL
PACKAGE SECURITY GUIDE
SENSITIVE INFORMATION

Version 8.0
July 1995

Information Systems Center
San Francisco, California

Introduction

Kernel's Sign-on/Security component provides security for all of DHCP. Security mechanisms include encryption of access and verify codes, hashing of electronic signatures, assignment of menu options, and allowing access to VA FileMan files. Most of these mechanisms are described in the Sign-On/Security chapter of the *Kernel Systems Manual*.

VA FileMan security codes set another layer of protection on the range of computing capability for each user. The VA FileMan access code is the string of characters stored in the variable DUZ(0). Programmer access to activities such as entering M code in VA FileMan fields is prohibited if DUZ(0) does not equal the at-sign (@). VA FileMan field and template access is also regulated. Devices may be restricted if the character string in the Security field of the Device file does not match the user's VA FileMan access code.

Access to files, previously controlled by the VA FileMan access code, can also be explicitly granted to each VA FileMan user as an attribute in the New Person file. This level of control becomes available when Kernel's File Access Security system is enabled. Six levels of access are possible: read, write, delete, LAYGO, data dictionary, and audit. For more information, see the *Kernel Security Tools Manual*, the File Access Security chapter of the *Kernel Systems Manual*, and the documentation for VA FileMan.

Kernel's menu options can be locked with security keys, have access prohibited by time of day or day of week, and have access temporarily prohibited with an out-of-order indicator. Assigning menu options is an activity that may be granted to application coordinators in a highly restricted way with the Secure Menu Delegation system. For more information on managing options and menus, see the Menu Manager: System Management chapter of the *Kernel Systems Manual*, and the *Kernel Security Tools Manual*.

Readers who wish to learn more about Kernel should consult these related manuals:

- *Kernel Installation Guide*
- *Kernel Release Notes*
- *Kernel Security Tools Manual*
- *Kernel Systems Manual*
- *Kernel Technical Manual*
- *MIRMO/ISC Operations Document*, Chapter 10 - DHCP Programming Standards and Conventions (SAC)
- *User's Guide to Computing*

Introduction

Security Keys

The security keys distributed with the Kernel are described below. See the VA FileMan and MailMan Technical Manuals for the keys that pertain to each.

PROVIDER	This key has the PERSON LOOKUP flag set so that an AK- cross reference is made in the New Person file for holders of this key. The PROVIDER key is a key given to entries in the New Person file that would have been added to the old Provider file. This key marks its holders as entries that are considered providers by some service in the hospital. For backward compatibility, if the provider key is given, then an entry is made in the Provider file; conversely, if a new entry is made to the Provider file, the New Person entry is given the PROVIDER key.
XQAL-DELETE	This key locks the Alerts for a User (Delete) [XQALERT BY USER DELETE] option. This option lets one user delete the alerts of another user. This option (and key) should only be made available to IRM personnel, and possibly some ADPACs.
XQSMDFM	This key locks the Limited File Manager Options (Build) option [XQSMD LIMITED FM] (under the Delegate's Menu Management menu). This option permits delegates to build some options based on VA FileMan templates.
XUARCHIVE	This key is needed to access the Archiving menu or to run any of the archiving options (For future use).
XUAUDITING	This key is needed to access VA FileMan's Auditing menu [DIAUDIT] or to run any of the Auditing options.
XUAUTHOR	This key allows the holder to edit all existing help frames, using '^E' when the frame is displayed, as well as allowing the holder to create new frames from within the menu system.
XUFILEGRAM	This key is needed to access VA FileMan's Filegram menu [DIFG] and to run any of the Filegram options.
XUMGR	This key is for users who need to act as site management staff. This also gives the user access to see information that is normally only available to the user that created it. A partial list of its use is: it allows its holders to create

"Routine"-type Options in the OPTION file with bracket syntax ([UCI]) for UCI-switching; it allows its holders to see the list of all spool file entries; it allows its holders to test options not on their menus.

- XUPROG** This key is needed to access the Programmer Options menu [XUPROG] from the Menu system. It also locks other programmer-oriented options, such as the Kernel Installation and Distribution System menu [XPD MAIN].
- XUPROGMODE** This key locks many programmer-oriented options, including the List Global [XUPRGL] and Programmer Mode [XUPROGMODE] options.
- XUSCREENMAN** This key is needed to access VA FileMan's ScreenMan menu (DDS SCREEN MENU).
- XUSPF200** This key allows special privileges in the NEW PERSON File. One privilege is that holders of this key don't have to enter a person's social security number when adding an entry to that file.
- ZTMQ** This key allows the user to change the status of tasks other than their own through Taskman Management's Dequeue Tasks, Requeue Tasks, and Delete Tasks options.

Kernel Locked Options

<u>Option Name</u>	<u>Locked By Key</u>
XPD INSTALLATION MENU	XUPROGMODE
XPD MAIN	XUPROG
XQALERT BY USER DELETE	XQAL-DELETE
XQSMD LIMITED FM OPTIONS	XQSMDFM
XUERTRP CLEAN	XUPROGMODE
XUPROG	XUPROG
XUPROGMODE	XUPROGMODE
XURESJOB	XUMGR
XUSERBLK	XUMGR
XUSESIG CLEAR	XUMGR

File Security

The table on the following pages lists the recommended file security settings for access to Kernel files.

Number	Name	DD	RD	WR	DEL	LAYGO	AUDIT
3	USER	#	#	#	#	#	
3.05	FAILED ACCESS ATTEMPTS LOG	@	@	@	@	@	
3.07	PROGRAMMER MODE LOG	@	@	@	@	@	
3.075	ERROR LOG	@	@	@	@	@	@
3.076	ERROR MESSAGES	@	@	@	@	@	@
3.081	SIGN-ON LOG	@	@	@	@	@	
3.1	TITLE	#			#		
3.2	TERMINAL TYPE	#		#	#	#	
3.22	DA RETURN CODES	@	@	@	@	@	@
3.23	LINE/PORT ADDRESS	@	@	@	@	@	@
3.5	DEVICE	#		#	#	#	
3.51	SPOOL DOCUMENT	@	@	@		@	
3.519	SPOOL DATA	@	@	@	@	@	@
3.54	RESOURCE	@	@	@	@	@	@
3.6	BULLETIN	#		#	#		
4	INSTITUTION			#	#		
4.1	FACILITY TYPE			#	#		
4.11	AGENCY	@		Y	@	@	@
4.3	KERNEL SITE PARAMETERS	@	#	#	#	#	
5	STATE	@	@	@	@	@	@
6	PROVIDER			#	#		
7	PROVIDER CLASS			#	#		
7.1	SPECIALITY			#	#		
9.2	HELP FRAME	#			#		#
9.4	PACKAGE	#		#	#	#	
9.6	BUILD	@	#	#	#	#	#
9.7	INSTALL	@	#	@	#	@	#
9.8	ROUTINE	#		#	#	#	
10	RACE			#	#		
11	MARITAL STATUS			#	#		
13	RELIGION			#	#		
14.4	TASKS	@		^	@	@	@
14.5	VOLUME SET	@	@	@	@	@	@
14.6	UCI ASSOCIATION	@	@	@	@	@	@
14.7	TASKMAN SITE PARAMETERS	@	@	@	@	@	@
14.8	TASK SYNC FLAG	@	@	@	@	@	@
16	PERSON	@	@	@	@	@	
19	OPTION	#		#	#	#	
19.081	AUDIT LOG FOR OPTIONS	@	#	#	#	#	#
19.1	SECURITY KEY	#	#	#	#	#	
19.2	OPTION SCHEDULING	@	#	#	@	@	@

File Security

(Continued)

Number	Name	DD	RD	WR	DEL	LAYGO	AUDIT
40.5	HOLIDAY	#	#	Dd	Dd	Dd	#
49	SERVICE/SECTION	#	D	d	d	d	
200	NEW PERSON	#		#	#		
8989.2	KERNEL PARAMETERS	@	@	@	@	@	@
8989.3	KERNEL SYSTEM PARAMETERS	@	#	@	@	@	
8991.5	XQAB ERRORS LOGGED	@	@	@	@	@	@
8992	ALERT	@	@	@	@	@	@
8992.1	ALERT TRACKING	@	@	@	@	@	@

Distribution of Kernel

To protect the security of DHCP systems, distribution of Kernel for use on any other computer system by DHCP sites is prohibited. All requests for copies of the Kernel for non-DHCP use should be referred to the DHCP site's local ISC.

Distribution of Kernel