training & documentation

SMART CARD

TB100 POWER PACK

User's Guide

PHILIPS

PHILIPS

TB100 POWER PACK

A publication of:

Philips Telecommunicatie en Data
Systemen Nederland B.V.
Systems Support - Training &
Documentation
P.O. Box 245
7300 AE Apeldoorn,
The Netherlands

Printed in The Netherlands, May 1990

The information contained in this publication is accurate to the best of Philips' knowledge. However, Philips disclaims any liability resulting from the use of this information and reserves the right to make changes without notice.

Order Number:	5122 995 52631
Manual Number:	Q40D

PREFACE

This manual explains how to use the software for the **TB100 Power Pack**. This training tool is designed for people with a theoretical knowledge of the TB100 Smart Card who wish to improve their practical understanding of the card.

- Chapter 1 explains the organisation of the manual and general use of the software
- Chapter 2 details the *Help* and *Grab* Functions
- Chapter 3 explains the menu-bar *Support* Functions
- Chapter 4 explains the *Power Tools* Functions
- Chapter 5 explains the *Index* Functions
- Appendix A explains the help system and how to customise it

WARNING

Please note that certain TB100 cards are delivered without the cryptographic inctructions *encrypt* and *decrypt*. For this reason, certain instruction sequences will not work on some cards. The passages in this manual dealing with these instructions are marked with the ❖ symbol.

Related Manuals
Q36D — TB100 Libraries Reference Manual
Q37D — TB100 Reference Manual
Q44D — TB100 Sample Applications

CONTENTS

LIST OF ILLUSTRATIONS

LIST OF TABLES

ONE INTRODUCTION

INSTALLATION

Hardware

Your hardware configuration must include:

- A workstation with one P3XXX computer (with either a hard disk and a diskette drive or two diskette drives) and one or two card-reader machines.
- The TB100 Power Pack diskette.
- At least one Philips TB100 Smart Card.

Saving The Training Application

To avoid accidentally destroying the TB100 Power Pack diskette, make a backup copy. Use this backup copy to run the system, and keep the original in a safe place, so extra backup copies can made, if necessary.

HARD-DISK SYSTEMS

If your computer has a hard disk, copy the TB100 Power Pack diskette onto it as follows:

- Insert the diskette in drive A:
- Make a directory on the hard disk ("PP", for example):

```
C:\>MD  PP RETURN
```

- Copy the contents of the diskette to the new directory:

```
C:\>COPY A:*.* C:\PP\*.* RETURN
```

TWO-FLOPPY SYSTEMS

If you don't have a hard disk, copy the Power Pack diskette onto a second diskette. The dialog will be as follows:

- Boot your computer from drive A:

- Run the MS-DOS Diskcopy program:

```
A:\>DISKCOPY A: B: RETURN
```

- You will see the following prompt:

```
     Insert source disk in drive A:
     Insert target disk in drive B:
     Strike any key when ready
```

- Insert the Power Pack diskette into drive A: and your blank diskette into drive B:. Press a key to start the copy process.

Following either these operations, store your Power Pack floppy diskette in a safe place, and use the copy to work on.

OPERATING PRINCIPLES

Running The Application

To start the application, type the following command:

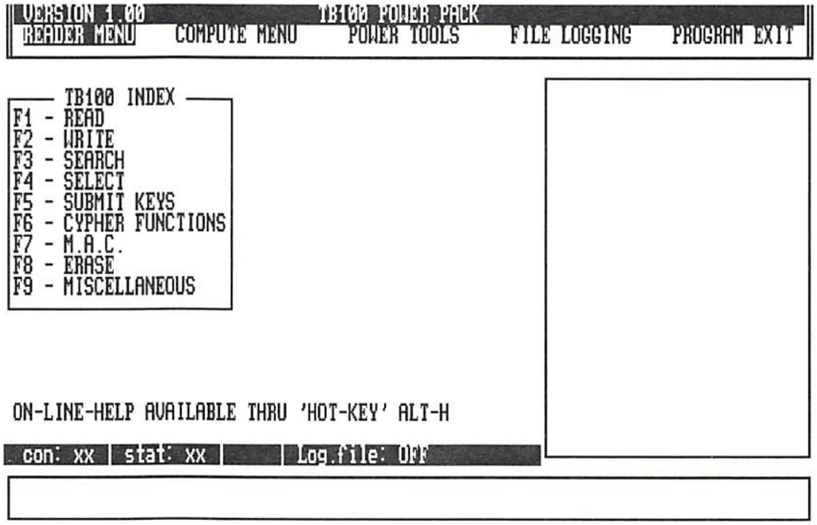
```
C:\PP>TB100PP/HELP RETURN
```

Adding the parameter "help" loads the HELP file. For more details, see Chapter 2.

Screen Layout

The screen looks like this:

FIGURE 1-01 MAIN SCREEN



ON-LINE-HELP AVAILABLE THRU 'HOT-KEY' ALT-H

con: xx | stat: xx | | Log.file: OFF

The screen is split into six fields:

1 A Menu-bar, for selecting individual menus

2 An Index, displaying function groups

3 A Communication window, displaying messages for you, the user

4 A Status line, containing:

- The connex status
- The driver status
- The name of the peripheral output used by the card reader (this is empty if output is not selected)
- the logging status and/or the name of the logging file (see Chapter 3)

5 The Data Entry window, where the data required by the functions is entered
6 The Display window, containing the results of calculations or messages from the card reader

Three other types of window are available when you run this software:

1 The Help window
2 The Error window
3 The View window

THE MENUS

The menu-bar has five menu selections:

- Reader Menu
- Compute Menu
- Power Tools
- File Logging
- Program Exit

When you start the application, the *Reader* menu is displayed automatically (in reverse video). To go into the *Reader* menu, just press RETURN.

To select another menu, use the ← and → keys to move the highlight to the menu you want. To go into the menu, press RETURN. To return to the menu-bar, press ESC.

Starting A Function

You can start a function in two ways:

1 The first method was explained above, and is summarised as:

  - Move the highlight on the menu-bar with the ← and → keys to the function you want
  - Press RETURN to enter the menu
  - Inside the menu, select with the ↓ and ↑
  - Press RETURN to enter the function

2 The second method gives you direct access to the function by typing a combination of keys. The combinations are of the SHIFT, CTRL, or ALT keys together with a function key. Entering the combination is by holding the special key down and then pressing the desired function key. If you need to use the "alternate" value of function key seven, for example, it will be shown in the text as ALT & F7.

Example Of Starting A Function

To access the *Close Log File* function:

- 1st method:
  - Select *File Logging* with the → key, then press RETURN.
  - Select *Close Log File* with the ↓ key and press RETURN.

- 2nd method:
  - Press the ALT & C keys together, as marked in front of the *Close Log File* entry in the *Logging* menu.

To Leave The Program

There are two ways of exiting the application:

- Use the → to select *program exit* from the menu-bar, and then press the RETURN key. Confirmation will be requested.

- Press the END key. This will take you directly to the confirmation stage of the function above.

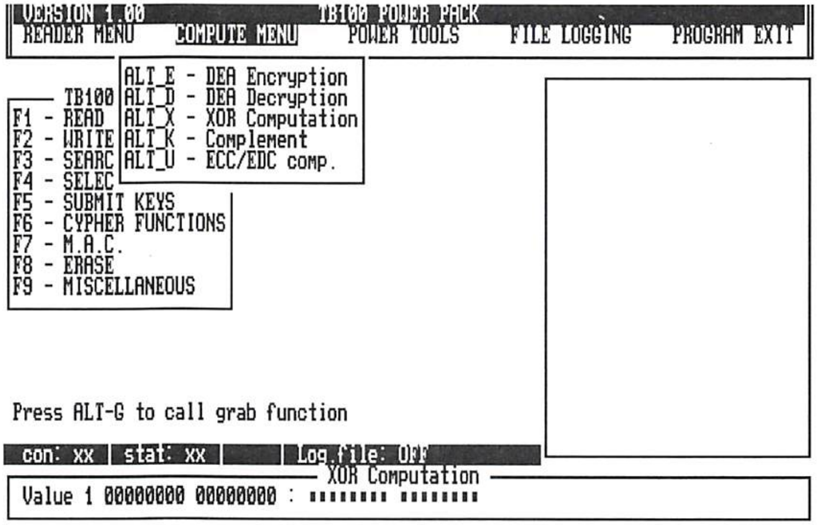
In either case, a confirmation box is displayed towards the bottom of the screen; to return to DOS, press "Y" (Yes).

Entering Parameters

You must set parameters in certain functions. In the example shown in Figure 1-02 the Input Window is active and you can:

- Type the parameters in, and press RETURN to enter them.
- Select from the parameters displayed in the Input Window, and then press the RETURN key.
- Enter the parameters during a work session by pressing ESC.

FIGURE 1-02 ENTERING A PARAMETER



```
VERSION 1.00                      TB100 POWER PACK
READER MENU     COMPUTE MENU      POWER TOOLS      FILE LOGGING      PROGRAM EXIT

            ALT_E - DEA Encryption
       TB100 ALT_D - DEA Decryption
F1 - READ   ALT_X - XOR Computation
F2 - WRITE  ALT_K - Complement
F3 - SEARC  ALT_U - ECC/EDC comp.
F4 - SELEC
F5 - SUBMIT KEYS
F6 - CYPHER FUNCTIONS
F7 - M.A.C.
F8 - ERASE
F9 - MISCELLANEOUS

Press ALT-G to call grab function

 con: xx  stat: xx          Log file: OFF
                                XOR Computation
 Value 1 00000000 00000000 : ........ ........
```

CAUTION

Data structure headers are entered by a different method - see the section on the *Power Tools* menu in Chapter 3.

Card Replies

Card replies are displayed in the Display window (see Figure 1-01, item 6). Depending on the instruction used, a prefix is attached to the result to clarify the source of the information.

TABLE 1-01 CALCULATION RESULT CODES

Code	Meaning
"Enc"	Encryption result.
"Dec"	Decryption result.
"MPC1"	Key-calculation result.
"XOR"	Result of an exclusive "OR".
Req	Data received from read result instruction.
p_stat	Card status word.
Add	Address data.
Cmpl	Result of calculating the complement of a number.
ECC/EDC	Result of an ECC/EDC calculation.
Hdr	Header creation within Power Tools menu.
Wrd	Word creation within Power Tools menu.

NOTE

Reading in a DF may not provide the information that you expect. Figure 1-03 shows part of the contents of a DF (the first fourteen words). If a read data instruction is issued with this DF just selected, for "0E" words from offset "00", only seven words will actually be reported. These are those in the right-hand column of the figure.

FIGURE 1-03 EXAMPLE LAYOUT

Phy. Adr.		Rel. Adr. & Meaning		Contents as read
"00"			WZ Header (word 1)	2F 00 00 05
"01"			WZ Header (word 2)	EF BF FF 23
"02"		"00"	WZ Body Words	
"03"		"01"		
"04"		"02"		
"05"			WZ Header (word 1)	2F 00 00 03
"06"			WZ Header (word 2)	93 EF FF 64
"07"		"00"	WZ Body Word	
"08"			SZ Header	0F 80 03 70
"09"		"00"	SZ Body Words	
"0A"		"01"		
"0B"			SZ Header	0C C0 03 31
"0C"		"00"	SZ Body Words	
"0D"		"01"		
"0E"			Virgin Word	FF FF FF FF

TWO HELP AND GRAB FUNCTIONS

THE HELP FUNCTION

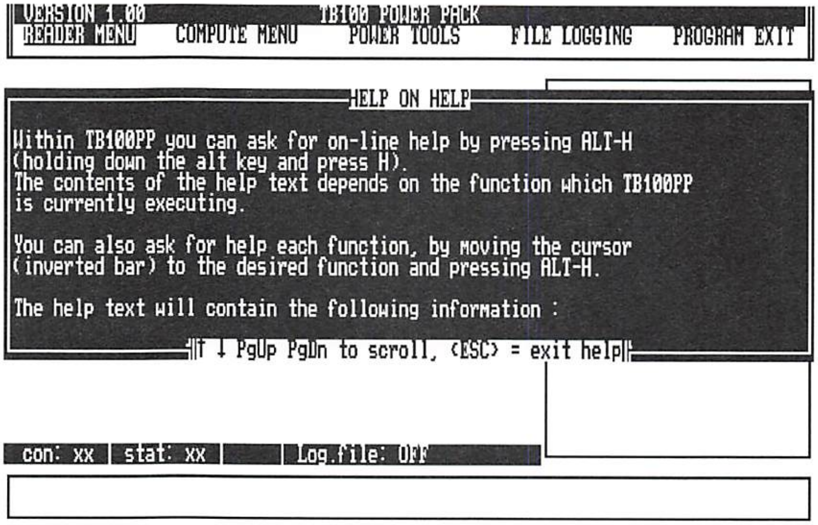
To obtain help, type ALT & H.

FUNCTION Provides access (at any time) to information on the current operation.

DISPLAY A Help window — see Figure 2-01.

PROCEDURE Move around the window using the ↑, ↓, PG UP, and PG DN keys.

FIGURE 2-01 HELP WINDOW



Within TB100PP you can ask for on-line help by pressing ALT-H
(holding down the alt key and press H).
The contents of the help text depends on the function which TB100PP
is currently executing.

You can also ask for help each function, by moving the cursor
(inverted bar) to the desired function and pressing ALT-H.

The help text will contain the following information :

↑ ↓ PgUp PgDn to scroll, <ESC> = exit help

NOTE

If you do not enter the Help file merge parameter while loading the TB100 Power Pack (see "Starting the Application" in Chapter 1), you will get a warning message ("*No help loaded. On-line help suppressed* "). To obtain the Help facilities, do the following:

- Exit from the application by pressing END followed by Y .
- Reload the software - using the full command:

```
C:\>TB100PP/HELP RETURN .
```

Help Files

The Help file can be translated or modified, by adding personal notes etc.

The file is written in ASCII format and has the name *TB100PP.HLP*. You can edit it with any ASCII editor.

You can find instructions on how to modify your help file in appendix A.

Remember to make a copy of the file before you modify it.

THE GRAB FUNCTION

FUNCTION

Grab enables you to copy parameters from the Display window to the Data Entry window. Only use this function during the entry of data.

INVOCATION

To use the Grab function, type ALT & G .

DISPLAY

A highlit bar appears in the Display window to identify the data which will be "grabbed".

PROCEDURE

A highlit bar is shown in the Display window. This bar can be moved over the data required by using the ↑ and ↓ keys. The RETURN key copies the highlit data to the Data Entry window.

To abort the Grab function, press the ESC key.

If the bar is highlighting a 64-bit (8-byte) value, different parts of this value may be selected. Repeated use of the TAB key will cycle the highlight position, illuminating the whole value, the last four bytes, and the first four bytes in turn.

If the parameter in the Display Window cannot be used in the Data Input window you will see the error message "*No grabbing data*".

READER MENU

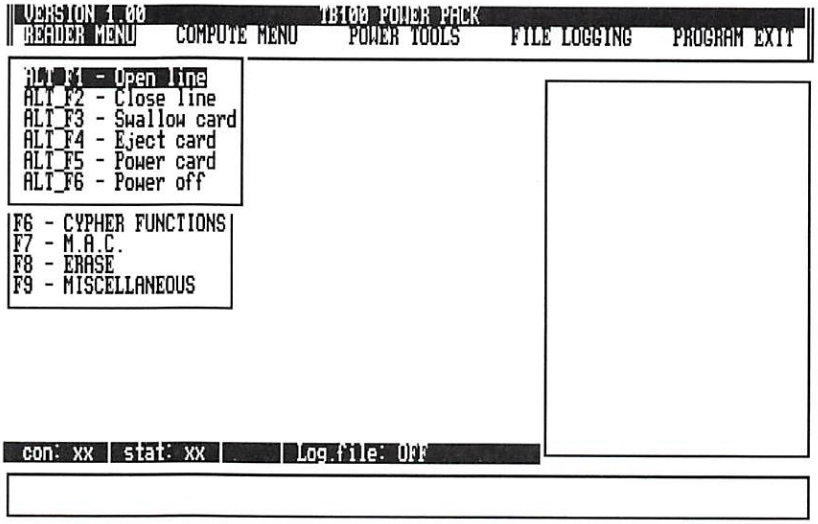
General

The reader menu is the first and the last menu used during a work session. It controls the logical connection to the card.

The available functions are:

- Open line
- Close line
- Swallow card
- Eject card
- Power card
- Power off

FIGURE 3-01 READER MENU



Open Line

FUNCTION

Opens the access path between the computer and the card reader. This function must be used before you do anything else.

INVOCATION - METHODS

- Type ALT & F1

- Select the *Open Line* option from the *Reader* menu.

PARAMETERS

Once the function is started the Data Entry window is opened and the following message appears:

```
Reader name : ■ ■ ■
```

Type the reader code (normally composed of two letters and a number), and press RETURN.

RESPONSE

If the line opens correctly, the reader name appears in the Status Line and a value of zero or above is shown in the *connex* ("con") and *status* ("status") fields.

If an error occurs, a value of "-1" is displayed for the *connex* value, and the corresponding error code is shown for the *status* field. Refer to the reference manual for your card reader for details.

NOTE

Up to 10 card-readers may be opened simultaneously. The command for the reader and card is sent to the last opened card-reader (as specified on the Status Line).

Close Line

FUNCTION Closes the data path opened by the "Open line" function.

INVOCATION METHODS

- Type ALT & F2
- Select the *Close Line* option from the *Reader* menu.

RESPONSE The reader name disappears from the Status Line and "-1" is displayed for the *connex* value. Multiple lines can be open at any time, although only one can be used. The lines are "stacked", so that closing the most recently opened line returns you to the previous one.

Swallow Card

FUNCTION Sends a signal to the card-reader to *Swallow* the card.

INVOCATION - METHODS

- Type ALT & F3
- Select the *Swallow Card* option from the *Reader* menu.

RESPONSE A status word (*p_stat*) is shown in the Display Window — see Table 3-01 below.

TABLE 3-01 SYSTEM STATUS WORD - SWALLOWING

Status word	**Meaning**
6080	Card swallowed correctly
6085	Card pulled out before swallowing completed
6086	Card jammed, or motor failure

For further information consult the reference manual for your card reader.

NOTE You must open the line before the card reader can *Swallow* a card.

Eject Card

FUNCTION

Stops the power supply to the card, and ejects the card from the card reader.

INVOCATION - METHODS

- Type [ALT] & [F4]
- Select the *Eject Card* option from the *Reader* menu.

RESPONSE

A status word (*p_stat*) is shown in the Display Window (see Table 3-02) and the card is ejected from the reader.

TABLE 3-02 SYSTEM STATUS WORD - EJECTION

Status word	**Meaning**
6080	Card ejected swallowed correctly
6086	Motor failure
6087	Card jammed

For further information consult the reference manual for your card reader.

Power Card

FUNCTION

Restarts a "mute" card (a card that has not been powered off and ejected).

INVOCATION - METHODS

- Type ALT & F5

- Select the *Power Card* option from the *Reader* menu.

RESPONSE

A status word (*p_stat*) is shown in the Display Window.

If the swallowed card is a TB100, you will see the following lines in the Display Window:

```
21 20 00 07 T5
SW1 SW2
```

This message is composed of:

- 21 20 00 07 — card signature; this must be "00 07" for a TB100 card
- T5 — state of the lock bits on the card
- SW1 — first byte of status word
- SW2 — second byte of status word

TABLE 3-03 T5 WORD

T5	Meaning:
20	The card is in the Personalisation phase — CDF does not yet exist
28	The card is in the Personalisation phase — CDF does exist
68	The card is in the Utilisation phase
68	The card may be in End-Of-Life phase, SW2 will indicate invalidity of CDF

TABLE 3-04 FIRST STATUS BYTE

Status word	Meaning
90	Valid access
97	Access Tracking Zone blocked from bad Issuer Key submission (IK, SK, or EK)
99	Two incorrect PIN's (or AID's) entered
9A	One incorrect PIN (or AID) entered
9F	Access Tracking Zone blocked from three consecutive bad Bearer Key submissions (PIN or AID)

For further information consult the reference manual for your card reader.

Power Off

FUNCTION

Stops the power supply to the card. Use this command to stop heat dissipation when the card is inoperative inside the card-reader.

INVOCATION - METHODS

- Type ALT & F6

- Select the *Power Off* option from the *Reader* menu.

For the *power_off* command, see TB100 Libraries Reference Manual.

RESPONSE

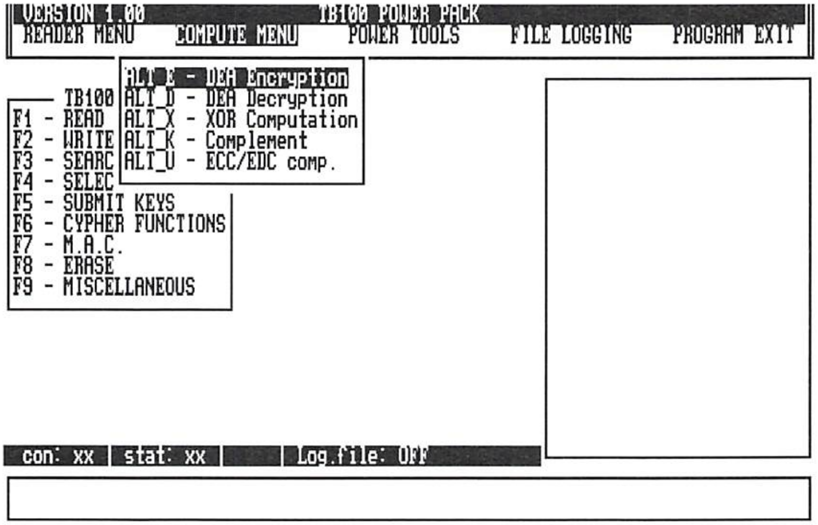
A status word (*p_stat*) is shown in the Display Window (see Table 3-01).

COMPUTE MENU

The Compute menu contains the functions for calculating parameters before inserting these parameters into the card. These include:

- Enciphering of data (the *DEA encryption* function)
- Deciphering of data (the *DEA decryption* function)
- Performing an exclusive OR between two bits of data (the *XOR Computation*) function
- Calculating the complement of a word (the *Complement* function)
- Calculating the ECC / EDC value of a string with a length of 1, 2, or 3 bytes (the *ECC / EDC Computation* function).

FIGURE 3-02 COMPUTE MENU



DEA Encryption

FUNCTION

Encrypts the eight data bytes by means of key input.

INVOCATION - METHODS

- Type ALT & E
- Select the *DEA Encryption* option from the *Compute* menu

PARAMETERS

Once the function is active, the first prompt appears in the Data Entry window:

```
Key 00000000 00000000: ■■■■■■■■■■■■■■■■
```

Enter all the bytes of the key. Once the key is entered, press RETURN and the next prompt will be displayed:

```
Data 00000000 00000000: ■■■■■■■■■■■■■■■■
```

Enter the data to be encoded (giving all the bytes).

RESPONSE

The calculation result is shown in the Display window, preceded by the abbreviation *Enc* (Encryption).

NOTE

If you press RETURN during data entry, the data recorded will be shown in the Display window.

DEA Decryption

FUNCTION

Decrypts the eight data bytes by means of key input.

INVOCATION - METHODS

- Type [ALT] & [D]
- Select the *DEA Decryption* option from the *Compute* menu.

PARAMETERS

When the function starts the first prompt appears in the Data Entry window:

```
Key 00000000 00000000: ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■
```

Enter all the bytes of the key. Once the key is entered, press [RETURN] and the second prompt will be displayed:

```
Data 00000000 00000000: ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■
```

Enter the data to be decoded (giving all the bytes).

RESPONSE

The calculation result is shown in the Display window, preceded by the abbreviation *Dec.*

NOTE

If you press [RETURN] during data entry, the data recorded will be shown in the Display window.

XOR Computation

FUNCTION

Executes an exclusive OR between two 8-byte values, allowing the calculation of parameters needed for certain instructions.

INVOCATION METHODS

- Type ALT & X
- Select the *XOR Computation* option from the *Compute* menu.

PARAMETERS

Once the function is active, the following prompt appears in the Data Entry window:

```
Value 1 00000000 00000000: ■■■■■■■■■■■■■■■■
```

Enter the first value, filling in all eight bytes. This must be in hex format. Then press RETURN. Next, enter the second value in the same way:

```
Value 1 xxxxxxxx xxxxxxxx Value 2 00000000 00000000: ■■■■■■■■■■■■■■■■
```

Once the data is entered, press RETURN again.

RESPONSE

The result is displayed in the Display window, preceded by the note *XOR*.

NOTE

If you press the RETURN key during data entry, the data recorded will be displayed in the Display Window.

Complement

FUNCTION

Calculates the complement of an eight-byte word.

INVOCATION - METHODS

Type ALT & K

- Select the *Complement* option from the *Compute* menu.

PARAMETERS

Once the function is started, the following prompt appears in the Data Entry window:

```
Value to be Complemented 00000000 00000000: ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■
```

Enter the word to be completed, giving all the bytes. Once the data is entered, press RETURN.

RESPONSE

The result is displayed in the Display window, preceded by the note *Cmpl.*

NOTE

If you press RETURN during data entry, the parameter recorded will be the result of the last operation.

ECC / EDC Computation

FUNCTION

Performs an ECC / EDC computation on a specified value. This value can be used to check the validity of data written inside the card.

INVOCATION - METHODS

- Type ALT & U

- Select the *ECC / EDC Computation* option from the *Compute* menu.

PARAMETERS

Once the function is started, the following prompt appears in the Data Entry window:

```
Length (in bytes) on which ECC / EDC needs to be computed : ■
```

You may enter "1", "2", or "3". The next prompt is:

```
Word on which ECC / EDC needs to be calculated: ■ ■ ■ ■ ■ ■
```

Enter the value upon which the ECC / EDC is to be calculated. Once the data is entered, press RETURN.

RESPONSE

The result is shown in the Display window, preceded by the note *ECC.*

NOTE

If you press RETURN during data entry, the parameter recorded will be the result of the last operation.

POWER TOOLS MENU

This menu is used to access a set of more sophisticated functions, where you can enter new data structures into the card EEPROM, and analyse those that already exist.

See Chapter 4 for the explanation of how to use the *Power Tools* menu.

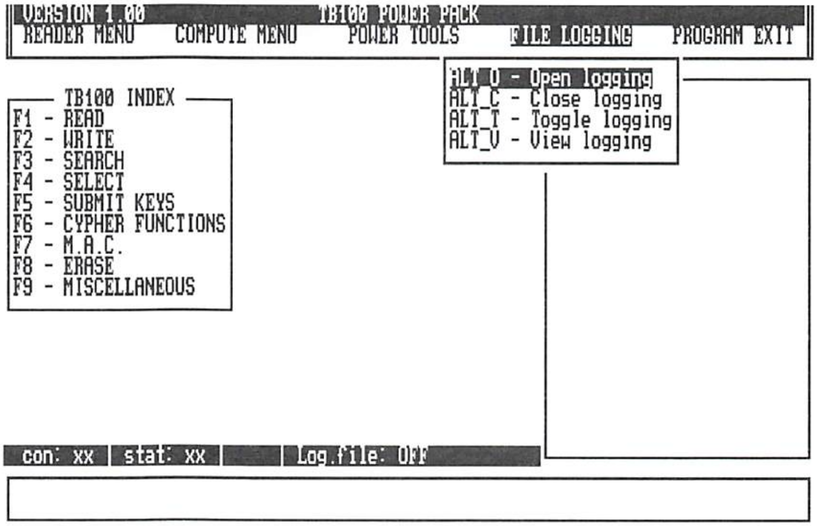
FILE LOGGING MENU

Use the File Logging menu to keep track of your work. When this function is active, everything you do is recorded in memory, then saved to your disk. You can then edit the file to analyse your work session.

The File Logging function offers you the following options:

- Start a record (*Open logging*)
- Stop a record (*Close logging*)
- Make a halt in a record (*Toggle logging*)
- Display the record (*View logging*)

FIGURE 3-03 FILE LOGGING MENU



```
VERSION 1.00                          TB100 POWER PACK
READER MENU   COMPUTE MENU   POWER TOOLS   FILE LOGGING   PROGRAM EXIT

                                          ALT_O - Open logging
  TB100 INDEX                             ALT_C - Close logging
F1 - READ                                 ALT_T - Toggle logging
F2 - WRITE                                ALT_V - View logging
F3 - SEARCH
F4 - SELECT
F5 - SUBMIT KEYS
F6 - CYPHER FUNCTIONS
F7 - M.A.C.
F8 - ERASE
F9 - MISCELLANEOUS

con: xx | stat: xx |     | Log.file: OFF
```

Open Log

FUNCTION

Starts sending information to the logging file.

INVOCATION - METHODS

Type ALT & O

- Select the *Open Log* option from the *File Logging* menu.

PARAMETERS

Once the function is started, the following prompt appears in the data-entry window:

```
Enter log filename:    ■ ■ ■ ■ ■ ■ ■ ■ <- max. 8 characters
```

Enter the name of your file. This filename is an ordinary MS-DOS filename, and must comply with the MS-DOS filename rules concerning length (between one and eight characters, inclusive) and content. For further information, consult your MS-DOS reference manual.

Do not try to enter the extension — this is automatically generated by the Power Pack software to avoid conflicts.

After typing in the filename, press RETURN. Your chosen filename will appear on the status line with the extension ".LGG".

NOTE

If you press RETURN without giving a file name, the file will be named *TB100PP.LGG* by the system.

The log file will be created in the logged directory. If the file already exists then the following message will be displayed:

```
Append logging data or Overwrite this file [<ESC> to abort]:
```

You can then choose from:

- A — to add to the end of the file that already exists
- O — to overwrite the file, destroying its current contents
- ESC — to abandon the function.

Close Log

FUNCTION Stops output of data to the logging file.

INVOCATION METHODS

- Type ALT & C

- Select the *Close Log* option from the *File Logging* menu.

PARAMETERS The system requests confirmation before stopping the logging process.

To stop output to the log file, press Y to confirm.

NOTE If you try to close a log file that has not been opened, an error message is displayed and you are exited from the function automatically.

Toggle Log

FUNCTION

Suspends or resumes output to a log file; it is not necessary to keep track of every operation done.

INVOCATION - METHODS

Type ALT & T

- Select the *Toggle Log* option from the *File Logging* menu.

PARAMETERS

The following message appears in the status line:

```
Log.file SUSPENDED.
```

Use this function if you want to stop recording in the log file for the time being. To re-start recording in the log file, simply toggle the function again.

View Log

FUNCTION

Displays the contents of a log file on the screen.

INVOCATION - METHODS

- Type ALT & V
- Select the *View Logging* option from the *File Logging* menu

PARAMETERS

You now have two options, depending on your previous actions:

- If there is a file already open, you will be prompted:

```
View Current log file or log file from Disk : ■
```

You may now choose from:
- C — to display the current file.
- D — to display another file from the disk. You will be prompted for the name of the file to be displayed, as described just below.

- If there is no file currently open, you must load a file, and you will see this prompt:

```
Enter Logfilename to be viewed : ■■■■■■■■
```

The procedure is identical to the *Open Log* function.

Once the file is displayed, you can move the cursor around the screen by using the cursor-control keys.

NOTES

- The logging file is also accessible from MS-DOS. You can edit the required file using any ASCII editor. The file is identified as *FileName.LGG*.
- If you want to print a logging file, issue the following MS-DOS command:

```
C:\>copy filename.lgg prn:
```

If this is the first time you have used the print command since the machine was re-started, MS-DOS will ask for the print device. Check that the printer is connected, switched on, and "on-line", and press RETURN.

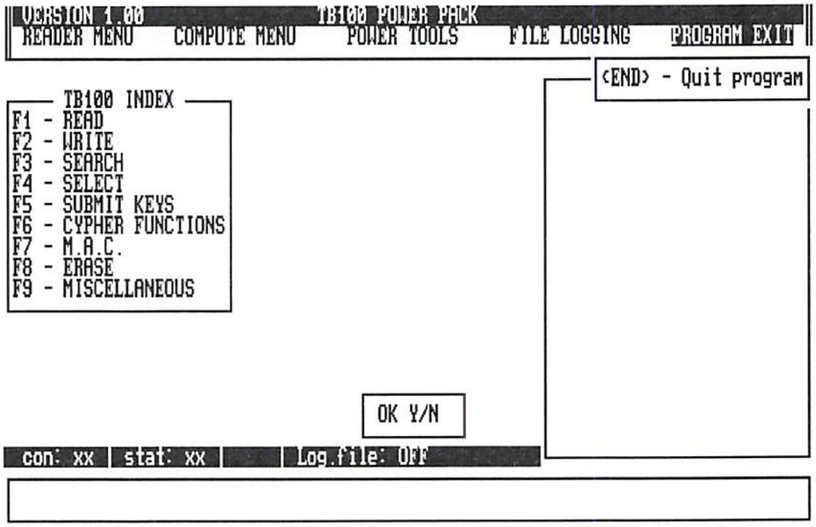
EXIT MENU

There are two ways in which to leave the program:

- Select the Exit menu. Select the only available choice in the menu — Leave Program — and answer Y to the confirmation prompt towards the bottom of the screen.

- Use the END key on the keypad. You must now confirm this action by answering Y to the confirmation prompt towards the bottom of the screen.

FIGURE 3-04 EXIT MENU



```
VERSION 1.00                TB100 POWER PACK
READER MENU   COMPUTE MENU   POWER TOOLS   FILE LOGGING   PROGRAM EXIT
                                                  <END> - Quit program
   TB100 INDEX
F1 - READ
F2 - WRITE
F3 - SEARCH
F4 - SELECT
F5 - SUBMIT KEYS
F6 - CYPHER FUNCTIONS
F7 - M.A.C.
F8 - ERASE
F9 - MISCELLANEOUS

                              OK Y/N
 con: xx | stat: xx |  | Log.file: OFF
```

FOUR POWER TOOLS

General

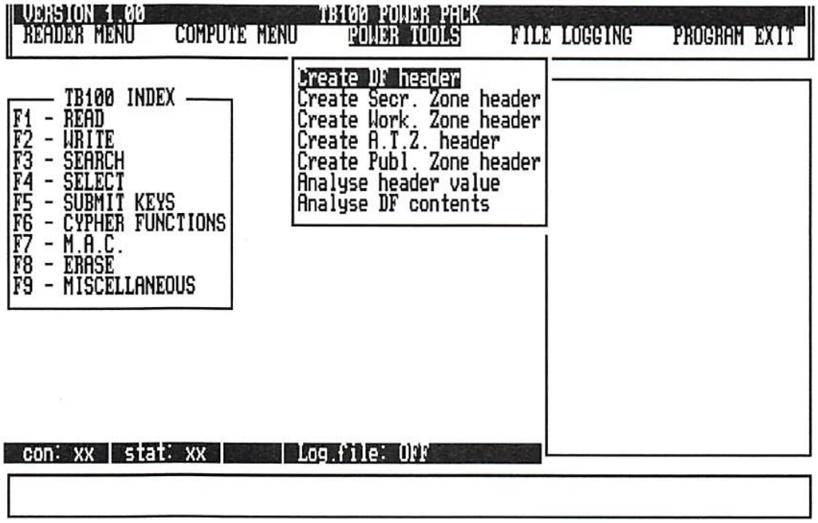
The *Power Tools* menu contains all the functions for working on headers.

With this facility, you can design and implement a card's architecture. That is:

- Create Data Files (DF)
- Create Secret Zones (SZ)
- Create Working Zones (WZ)
- Create Access Tracking Zone (ATZ)
- Create Public Zones (PZ)

Functions are also available for analysing the headers you have created.

FIGURE 4-01 POWER TOOLS MENU



Screens

The data-entry screens for composing the data structure headers are divided into four parts:

- Header Content display. This shows, in both binary and hexadecimal, the content of the header that you are designing. In other words, this is the bit-pattern that would be written if you press the F10 key.

- Header Field Name display. This is a list of each of the data fields in the header.

- Field Content display. To the right of the Header Field Name display, this area shows the current content of the field in a more symbolic fashion.

- Prompt area. This displays the method of using the part of the screen currently occupied by the cursor (see below).

Usage

On selecting a screen for data entry, regardless of the header to be entered, the following rules apply:

- You enter the screen with the cursor positioned on the top field-name in the Header Field Name display. You may move from one name to another using the ↑ and ↓ keys. As you move from field to field, the corresponding bits in the binary part of the Header Content display will flash.

- Place the highlight bar over the name of the field to be changed and then press RETURN to move the cursor into the Field Content display area.

- There are three ways in which a field may be given a value, depending on the type of field:
  - Numeric values. These are entered with the keyboard number keys. The value present at the start of creation will be the default value. This is usually the minimum legal value. An example of this type of field is the *length* field of a header.
  - Choice list. In some cases, a choice list is shown, and you select from this using the ← and → keys. An example of this is the *level* field of a header.
  - Choice list. In other cases, a default choice is shown. If another choice is made, using the ↑ and ↓ keys, a selection box is displayed. Examples of this are the creations fields in the *DF Creation* screen.

  After selecting the correct value for the field, the RETURN key returns the cursor to the Header Field Name display area.

Writing A Header

For all screens, the F10 key is used to send the completed header data to the card. You are presented with a selection box with three choices:

HOW TO WRITE

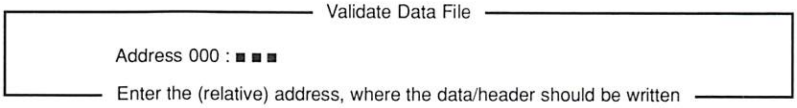
- *create DF or Zone*
- *secure write header by IK*
- *secure write header by SK*

These are the three possible ways of writing a header to the card, and you choose one of these, using the cursor control keys and the RETURN key.

WHERE TO WRITE

Next, you are requested for the location of the new structure.

FIGURE 4-02 STRUCTURE POSITION



Validate Data File

Address 000 : ■ ■ ■

Enter the (relative) address, where the data/header should be written

If you chose to use the *create DF or Zone* instruction, the operation will now proceed. The other two instructions, however, require more information. In either case, the dialogue will continue with a request for the first two bytes of the Current Data Structure:

DATA FILE I.D.

```
2 first bytes : ■ ■ ■ ■
```

KEY KRP

Next, if you have elected to use an SK, you must provide the Key Reference Pattern (KRP) of the key that you wish to use:

```
Key Reference Pattern : ■ ■ ■ ■
```

SK

Now, the value of the key itself must be entered. For example, with the SK key, the prompt will be:

```
SK 00000000 00000000 : ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■
```

RANDOM

Finally, you must provide the value of the last-generated random number (with a *generate random* instruction: see the *compute* menu):

```
Ran. 00000000 00000000 : ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■
```

After you have confirmed the operation, the data will be written to the card.

For the last two numbers the Grab function described in Chapter 2 is available. However, if several operations have been carried out since the generation of the last random number, it may no longer be visible on-screen. It is always advisable, to make a note of this number elsewhere.

Create DF Header

FUNCTION

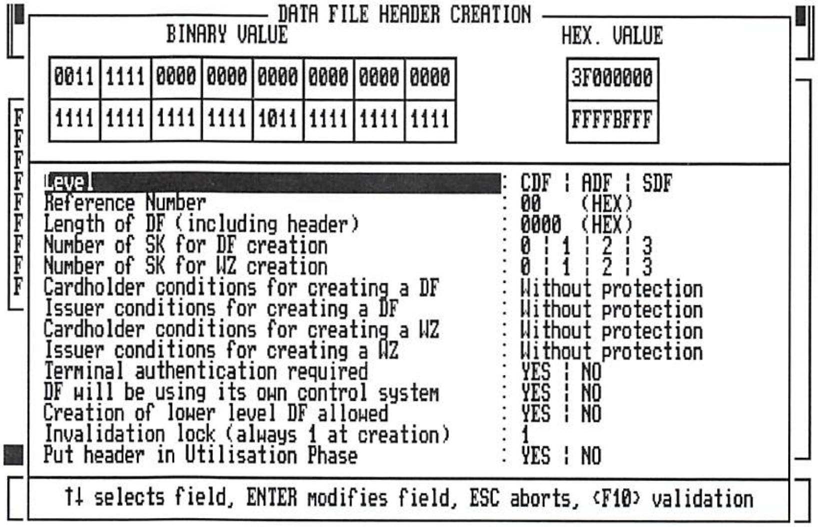
Enables you to create the header of a DF of level one, two or three.

INVOCATION

Select the *Create DF Header* option from the *Power Tools* menu

After choosing the option, the following screen appears:

FIGURE 4-03 CREATE DF HEADER



```
                     DATA FILE HEADER CREATION
             BINARY VALUE                               HEX. VALUE

 0011 1111 0000 0000 0000 0000 0000 0000                 3F000000
 1111 1111 1111 1111 1011 1111 1111 1111                 FFFFBFFF

 Level                                       : CDF ¦ ADF ¦ SDF
 Reference Number                            : 00    (HEX)
 Length of DF (including header)             : 0000  (HEX)
 Number of SK for DF creation                : 0 ¦ 1 ¦ 2 ¦ 3
 Number of SK for WZ creation                : 0 ¦ 1 ¦ 2 ¦ 3
 Cardholder conditions for creating a DF     : Without protection
 Issuer conditions for creating a DF         : Without protection
 Cardholder conditions for creating a WZ     : Without protection
 Issuer conditions for creating a WZ         : Without protection
 Terminal authentication required            : YES ¦ NO
 DF will be using its own control system     : YES ¦ NO
 Creation of lower level DF allowed          : YES ¦ NO
 Invalidation lock (always 1 at creation)    : 1
 Put header in Utilisation Phase             : YES ¦ NO

   ↑↓ selects field, ENTER modifies field, ESC aborts, <F10> validation
```

When all the parameters of the header are set to your satisfaction, press the F10 key to indicate that you have finished designing the header. You are then prompted for the function to use to write the header to the card.

PARAMETERS

As you select each field, the corresponding part of the binary display in the main menu flashes. As you type in the parameters, the changes are incorporated in the menu.

The control panel has fourteen fields; these are:

- Level — Enter the level of the DF. Use the ← and → keys to select the level (CDF, ADF or SDF) and then press RETURN.

- Reference Number — Enter the reference number of the DF (this number is, in effect the title of the DF): this must be between "00" and "FF", inclusive. Once entered, press RETURN.

- Length of DF — Enter the length of the DF (four hexadecimal digits). This must cover the length of DF body plus length of header (2 words).

- Number of SK for DF Creation — Enter the binary-coded number of the SK allowing creation of one or more secret zones in the DF.

- Number of SK for WZ Creation — Enter the binary-coded number of the SK protecting creation of the WZ.

- Cardholder conditions for creating a DF — as soon as you select this field, a selection box appears, offering the following options:

  - Without protection
  - Either PIN or AID
  - Both PIN and AID

  Select your option using the ↑ and ↓ keys and press RETURN.

- Issuer conditions for creating a DF — As soon as you select this field, a selection box appears offering the following options:

  - Without protection
  - Authentication by IK
  - Secure write by SK
  - Auth. + sec. write by IK

  Select your option using the ↑ and ↓ keys and press RETURN.

- Cardholder conditions for creating a WZ — As soon as you select this field, a selection box appears offering the following options:

  - Without protection
  - Either PIN or AID
  - Both PIN and AID

  Select your option using the ↑ and ↓ keys and press RETURN.

- Issuer conditions for creating a WZ — As soon as you select this field, a selection box appears offering the following options:

  - Without protection
  - Authentication by IK
  - Secure write by SK
  - Auth. + sec. write by IK

  Select your option using the ↑ and ↓ keys and press RETURN.

- Terminal authentication required — Prompt asking if the AK needs to be requested before any security instructions are issued. Make your selection using the ← and → keys and press RETURN.

- DF will be using its own control system — Prompt asking if the DF being created uses its CS or the CS of the higher level DF. Select YES or NO using the ← and → keys and press RETURN. In the case of a DCF, the reply can only be YES.

- Creation of lower-level DF allowed — Prompt asking whether a lower level DF can be created. Select YES or NO using the ← and → keys and press RETURN. In the case of an SDF, the reply can only be NO.

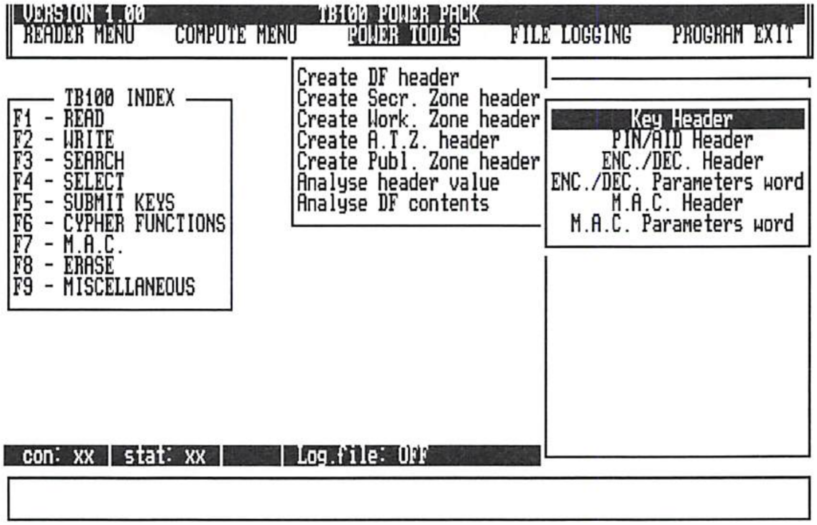
- Invalidation lock — Prompt asking whether the DF being created is invalid. Leave this byte at "1" during the creation phase.

- Put header in Utilisation Phase — Prompt asking into which phase the DF should go after creation. Select YES or NO using the ← and → keys and press RETURN. If NO is selected, the DF will remain in Personalization Phase.

Creating Secret Zones - General

On selecting the option to create a Secret Zone header from the Power Tools menu, you must select what kind of header you wish to create, as there are several kinds of Secret Zone. In addition, some of these are extended by special areas within the zone itself, and this menu (see below) allows you to select which kind of Secret Zone structure you wish to create.

FIGURE 4-04 CHOICE OF SECRET ZONE



Create Secret Zone - Key Header

FUNCTION

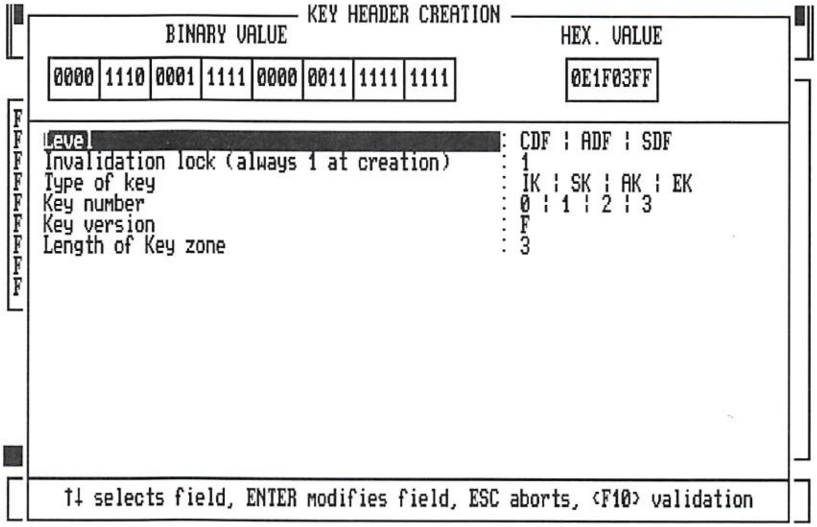
Enables you to create the header of a Secret Zone of the type used for storing key values.

INVOCATION

Use the *Key Header* function in the *SZ Creation* option of the *Power Tools* menu

After starting the function, the following screen appears:

FIGURE 4-05 CREATE KEY HEADER



```
                              KEY HEADER CREATION
            BINARY VALUE                                       HEX. VALUE

 0000|1110|0001|1111|0000|0011|1111|1111                        0E1F03FF

 Level                                                   : CDF ¦ ADF ¦ SDF
 Invalidation lock (always 1 at creation)                : 1
 Type of key                                             : IK ¦ SK ¦ AK ¦ EK
 Key number                                              : 0 ¦ 1 ¦ 2 ¦ 3
 Key version                                             : F
 Length of Key zone                                      : 3

      ↑↓ selects field, ENTER modifies field, ESC aborts, <F10> validation
```

When all the parameters of the header are set to your satisfaction, press the F10 key to indicate that you have finished designing the header. You are then prompted for the function to use to write the header to the card.

PARAMETERS

As you select each field, the corresponding part of the binary display in the main menu flashes and, as you type in the parameters, the changes are incorporated in this display.

The screen contains six fields, with which the following data may be entered:

- Level — Enter the level of the DF. Use the ← and → keys to select the level (CDF, ADF or SDF), then press RETURN.
- Invalidation lock — Prompt asking whether the header being created is invalid. Leave this byte at "1" during the creation phase.
- Type of key — Specify the type of key you wish to use the Secret Zone for (via the ← and → keys), then press RETURN.
- Key number — Use the ← and → keys to select the key number. This field does not operate for the IK header, since there can only be one IK.
- Key version — enter the key version. May be between "0" and "F", inclusive.
- Length of key — Enter the length of the zone allocated to the key, using a single hexadecimal digit. The length must cover the length of body plus the length of the header (1 word). If you press RETURN only, a length of three words will be entered by default.

Create Secret Zone: PIN/AID Header

FUNCTION

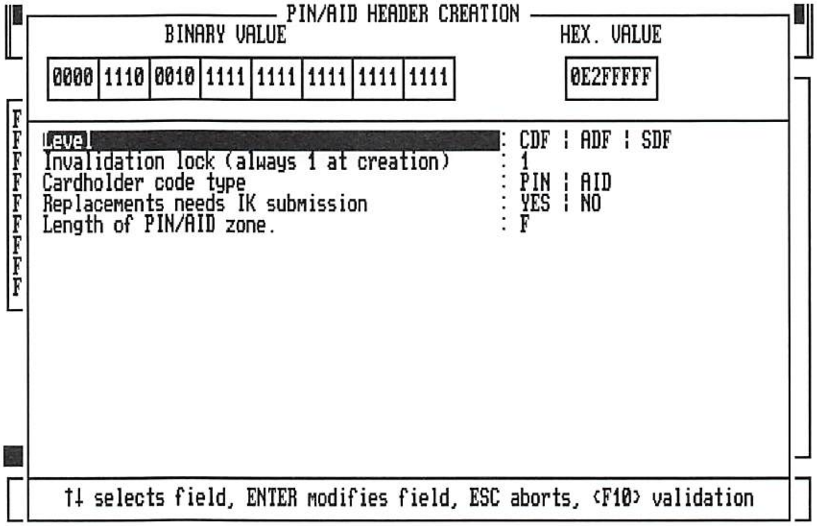
Enables you to create headers for the PIN and the AID's.

INVOCATION

Select *PIN / AID Header* from the *SZ Creation* option in the *Power Tools* menu.

After starting the function, the following screen appears:

FIGURE 4-06 CREATE PIN / AID SECRET ZONE HEADER



```
                          PIN/AID HEADER CREATION
              BINARY VALUE                                 HEX. VALUE

 |0000|1110|0010|1111|1111|1111|1111|1111|                 |0E2FFFFF|

F
F  Level                                       : CDF ¦ ADF ¦ SDF
F  Invalidation lock (always 1 at creation)    : 1
F  Cardholder code type                        : PIN ¦ AID
F  Replacements needs IK submission            : YES ¦ NO
F  Length of PIN/AID zone.                     : F
F
F
F

  ↑↓ selects field, ENTER modifies field, ESC aborts, <F10> validation
```

When all the parameters of the header are set to your satisfaction, press the F10 key to indicate that you have finished designing the header. You are then prompted for the function to use to write the header to the card.

As you select each field, the corresponding part of the binary display in the main menu flashes. As you type in the parameters, the changes are incorporated into the menu.

The control panel comprises five fields, into which data are entered as follows:

- Level — Enter the level of the header. Use the ← and → keys to select the level (CDF, ADF or SDF); then press RETURN.

- Invalidation lock — Prompt asking whether the header being created is invalid. Leave this byte at "01" during the creation phase.

- Cardholder code type — This prompt asks for the type of access code for this header: select between PIN and AID using the ← and → keys) then press RETURN.The selection "PIN" is only valid for a CDF-level header.

- Replacements need IK submission — Prompt asking if the IK will control changes of PIN. Select between YES and NO using the ← and → keys and then press RETURN.

- Length of key version — Enter the length of the zone allocated to the PIN (or the AID), using a single hexadecimal digit. This length must cover the length of the body plus the length of the header (1 word).

  If you press RETURN only, the value "E" will be entered by default, giving enough room for six changes of PIN (or AID).

Create Secret Zone ENC. / DEC. Header

FUNCTION

To create headers for Secret Zones for encode and decode keys.

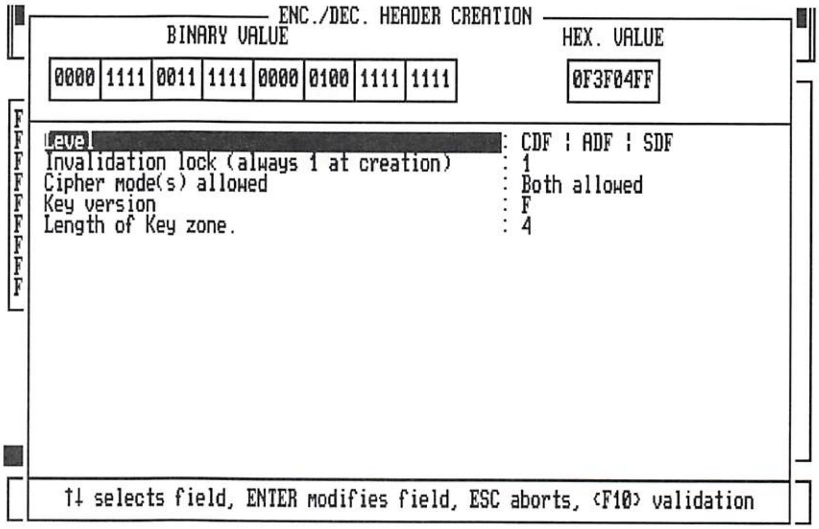
INVOCATION

Select *ENC. / DEC. Header* from the *SZ Creation* option in the *Power Tools* menu.

PARAMETERS

After starting the function, the following window appears:

FIGURE 4-07 CREATE ENC. / DEC. HEADER



```
ENC./DEC. HEADER CREATION
BINARY VALUE                                              HEX. VALUE
0000 1111 0011 1111 0000 0100 1111 1111                   0F3F04FF

Level                                    : CDF ¦ ADF ¦ SDF
Invalidation lock (always 1 at creation) : 1
Cipher mode(s) allowed                   : Both allowed
Key version                              : F
Length of Key zone.                      : 4

↑↓ selects field, ENTER modifies field, ESC aborts, <F10> validation
```

When all the parameters of the header are set to your satisfaction, press the F10 key to indicate that you have finished designing the header. You are then prompted for the function to use to write the header to the card.

As you select each field, the corresponding part of the binary display in the main menu flashes. As you enter the parameters, the changes are incorporated in the menu.

The control panel comprises five fields:

- Level — Enter the level of the header. Use the [←] and [→] keys to select the level (CDF, ADF or SDF); then press [RETURN].

- Invalidation lock — This prompt asks you if the header being created is invalid. Leave this byte at "01" during the creation phase.

- Cipher mode(s) allowed — Prompt requesting the direction of the operation: As soon as you select this field, a window appears offering the following options:

  - Encryption only
  - Decryption only
  - Both allowed.

  Select using the [↑] and [↓] keys and then press [RETURN].

- Key version — Enter the number of the version of the key; this lies in the range "0" to "F", inclusive.

- Length of key zone — Enter the size of the secret zone that will contain the header and the body. This must be in hexadecimal, and between "1" and "F". If you press [RETURN] only, a value of "04" will be entered automatically.

NOTE

A zone capable of storing one key must have a length of at least three words (one for the header and two for the key).

Create Secret Zone: ENC. / DEC. Parameters Word

FUNCTION

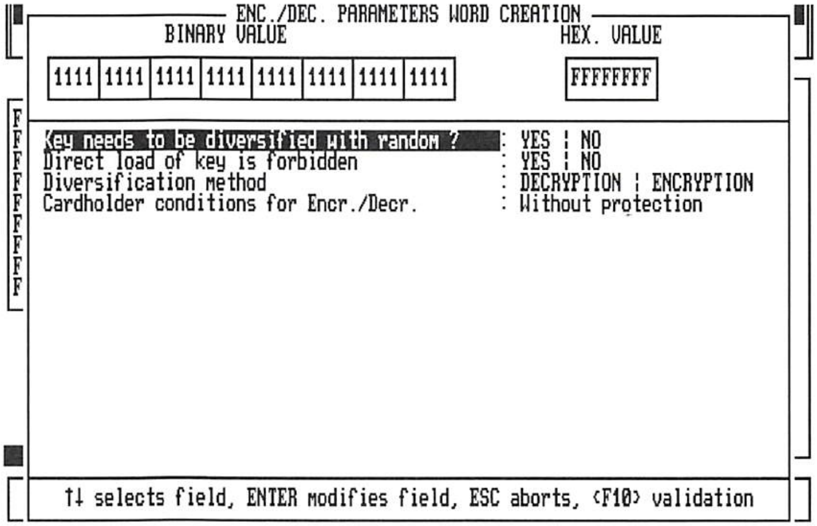
To create the parameter word for encoding / decoding Secret Zones.

INVOCATION

Select *ENC. / DEC. Parameters Word* from the *SZ Creation* option in the *Power Tools* menu.

After starting the function, the following screen appears:

FIGURE 4-08 CREATE ENC. / DEC. PARAMETERS WORD



```
                 ENC./DEC. PARAMETERS WORD CREATION
        BINARY VALUE                                  HEX. VALUE

 1111|1111|1111|1111|1111|1111|1111|1111               FFFFFFFF

 Key needs to be diversified with random ?   : YES ¦ NO
 Direct load of key is forbidden             : YES ¦ NO
 Diversification method                      : DECRYPTION ¦ ENCRYPTION
 Cardholder conditions for Encr./Decr.       : Without protection

   ↑↓ selects field, ENTER modifies field, ESC aborts, <F10> validation
```

When all the parameters of the header are set to your satisfaction, press the F10 key to indicate that you have finished designing the header. You are then prompted for the function to use to write the header to the card.

As you select each field, the corresponding part of the binary display in the main menu flashes and as you enter the parameters, the changes are incorporated in the menu.

The control panel comprises four fields;

- Key needs to be diversified with random — Use the [←] and [→] keys to select between YES and NO, then press [RETURN].

- Direct load of key is forbidden — This prompt asks what key must be used in the EEPROM as an encryption/decryption key. Use the [←] and [→] keys to select between YES and NO, then press [RETURN].

- Diversification method — This prompt requests which diversification method you wish to use. Use the [←] and [→] keys to select between Encryption and Decryption, then press [RETURN].

- Cardholder conditions for encr./decr. — This prompt requests conditions under which cardholder can use the Encryption and Decryption system. As soon as you select this field, a window appears with the following options:

  - Without protection
  - Either PIN or AID
  - Both PIN and AID

  Select your option using the [↑] and [↓] keys to select between YES and NO, then press [RETURN].

Create Secret Zone: MAC Header

FUNCTION

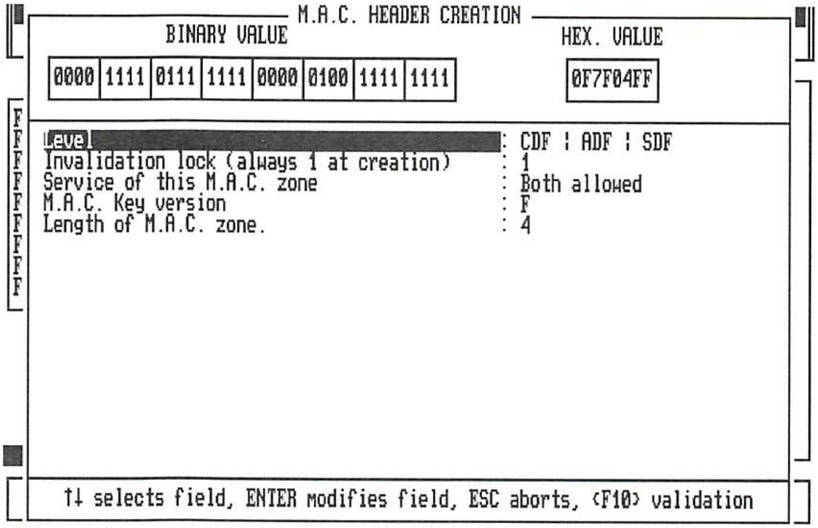
This function enables you to create headers for the MAC Secret Zones.

INVOCATION

Select *MAC Header* from the *SZ Creation* option in the *Power Tools* menu.

After starting the function, the following screen appears:

FIGURE 4-09 CREATE MAC HEADER



```
                          M.A.C. HEADER CREATION
             BINARY VALUE                                  HEX. VALUE
 0000 1111 0111 1111 0000 0100 1111 1111                    0F7F04FF

 Level                                        : CDF ¦ ADF ¦ SDF
 Invalidation lock (always 1 at creation)     : 1
 Service of this M.A.C. zone                  : Both allowed
 M.A.C. Key version                           : F
 Length of M.A.C. zone.                       : 4

   ↑↓ selects field, ENTER modifies field, ESC aborts, <F10> validation
```

When all the parameters of the header are set to your satisfaction, press the F10 key to indicate that you have finished designing the header. You are then prompted for the function to use to write the header to the card.

As you select each field, the corresponding part of the binary display in the main menu flashes. As you enter the parameters, the changes are incorporated in the menu.

The control panel comprises six fields:

- Level — Enter the level of the header. Use the ← and → keys to select between YES and NO, then press RETURN.

- Invalidation lock — This prompt asks if the header being created is invalid. Leave this byte at "01" during the creation phase.

- Service of this MAC zone — This prompt requests if the zone is used for generation or verification, or both; when you select this field, a window appears offering the following options:

    - Generation only
    - Verification only
    - Both allowed

  Select using the ← and → keys and press RETURN.

- MAC key version — Enter the number of the key version. This must be between "0" and "F".

- Length of MAC zone — Enter the size of the zone that will contain the header, using hexadecimal coding. This must be between "1" and "F". If you press RETURN only, a value of "4" is entered automatically.

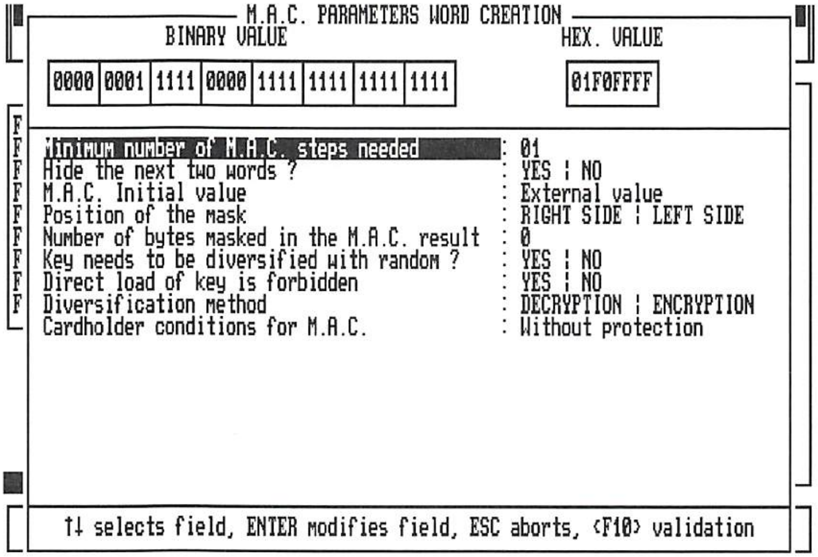
Create Secret Zone: MAC Parameters Word

FUNCTION To create parameter words for a MAC Secret Zone.

INVOCATION Select *MAC Parameters Word* from the *SZ Creation* option in the *Power Tools* menu.

After starting the function, the following screen appears:

FIGURE 4-10 CREATE MAC PARAMETERS WORD



```
                     M.A.C. PARAMETERS WORD CREATION
          BINARY VALUE                                    HEX. VALUE

 0000 0001 1111 0000 1111 1111 1111 1111                   01F0FFFF

 Minimum number of M.A.C. steps needed        : 01
 Hide the next two words ?                    : YES ¦ NO
 M.A.C. Initial value                         : External value
 Position of the mask                         : RIGHT SIDE ¦ LEFT SIDE
 Number of bytes masked in the M.A.C. result  : 0
 Key needs to be diversified with random ?    : YES ¦ NO
 Direct load of key is forbidden              : YES ¦ NO
 Diversification method                       : DECRYPTION ¦ ENCRYPTION
 Cardholder conditions for M.A.C.             : Without protection

   ↑↓ selects field, ENTER modifies field, ESC aborts, <F10> validation
```

When all the parameters of the header are set to your satisfaction, press the F10 key to indicate that you have finished designing the header. You are then prompted for the function to use to write the header to the card.

As you select each field, the corresponding part of the binary display in the main menu flashes. As you enter the parameters, the changes are incorporated in the menu.

The screen contains nine header fields:

- Minimum number of MAC steps needed — Enter the minimum number of iterations required for obtaining the MAC result.

- Hide the next two words — Asks if the two words coming after the parameter word should be hidden. Use the ← and → keys to select between YES and NO, then press RETURN.

- MAC initial value — Enter the value of the initial MAC value. When you select this field, a window appears with the following options:

  - Internal value
  - Counter
  - Random number
  - External value

  Select your option using the ↑ and ↓ keys and press RETURN.

- Position of the mask — Enter the part of the MAC message to be hidden. Select between LEFT SIDE and RIGHT SIDE using the ← and → keys to select between YES and NO, then press RETURN.

  If you select LEFT SIDE, the most significant bytes will be masked.

- Number of bytes masked in the MAC — Enter the number of bytes to be masked during the MAC result. They must be between "0" and "7".

- Key needs to be diversified with random — This prompt asks if the MAC key needs to be "diversified" by a random number. Use the ← and → keys to select between YES and NO and then press RETURN.

- Direct load of key is forbidden — This prompt asks if the key in the EEPROM can be used directly as a MAC key. Use the ← and → keys to select between YES and NO and then press RETURN.

- Diversification method — This prompt asks which diversification method you want to use. Use the [←] and [→] keys to select between Encryption and Decryption, and then press [RETURN].

- Cardholder conditions for MAC — Asks the conditions under which cardholder can use the MAC. As soon as you select this field, a window appears offering the following options:

  - Without protection
  - Either PIN or AID
  - Both PIN and AID

  Select your option using the [↑] and [↓] keys and press [RETURN].

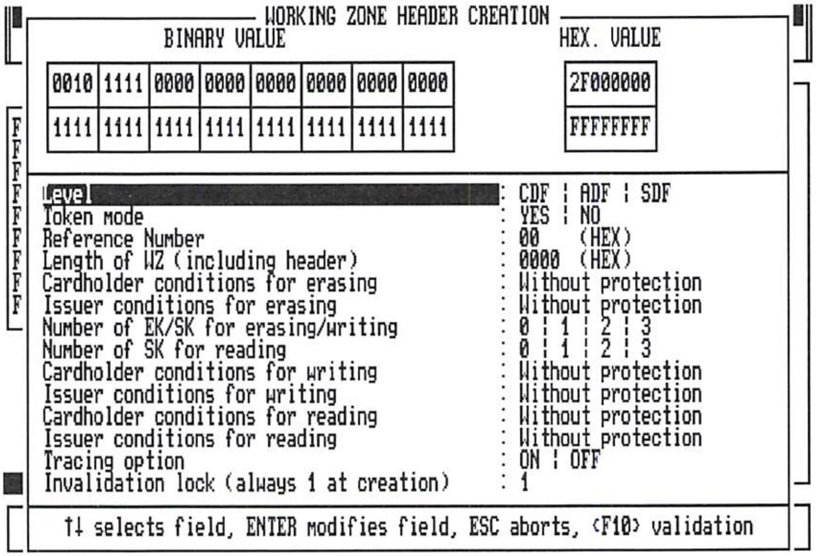
Create Working Zone Header

FUNCTION Used to create a header for a working zone.

INVOCATION Select *Create Work. Zone Header* from the *SZ Creation* option in the *Power Tools* menu.

After starting the function, the following screen appears:

FIGURE 4-11 CREATE W.Z. HEADER



```
                      WORKING ZONE HEADER CREATION
              BINARY VALUE                                 HEX. VALUE

 0010|1111|0000|0000|0000|0000|0000|0000                   2F000000
 1111|1111|1111|1111|1111|1111|1111|1111                   FFFFFFFF

 Level                                    : CDF ¦ ADF ¦ SDF
 Token mode                               : YES ¦ NO
 Reference Number                         : 00   (HEX)
 Length of WZ (including header)          : 0000 (HEX)
 Cardholder conditions for erasing        : Without protection
 Issuer conditions for erasing            : Without protection
 Number of EK/SK for erasing/writing      : 0 ¦ 1 ¦ 2 ¦ 3
 Number of SK for reading                 : 0 ¦ 1 ¦ 2 ¦ 3
 Cardholder conditions for writing        : Without protection
 Issuer conditions for writing            : Without protection
 Cardholder conditions for reading        : Without protection
 Issuer conditions for reading            : Without protection
 Tracing option                           : ON ¦ OFF
 Invalidation lock (always 1 at creation) : 1

    ↑↓ selects field, ENTER modifies field, ESC aborts, <F10> validation
```

When all the parameters of the header are set to your satisfaction, press the F10 key to indicate that you have finished designing the header. You are then prompted for the function to use to write the header to the card.

As you select each field, the corresponding part of the binary display in the main menu flashes. As you enter the parameters, the changes are incorporated in the menu.

The control panel comprises fourteen fields:

- Level — Enter the level of the header. Use the ← and → keys to select the level (CDF, ADF or SDF), then press RETURN.

- Token mode — Requests whether the zone will be used for token mode operations. Use the ← and → keys to select between YES and NO, then press RETURN.

- Reference number — Requests the reference number of the zone (= title); this must be between "00" and "FF". Confirm with the RETURN key.

- Length of working zone — Enter the length of the working zone, over two bytes hexadecimal. Length must include lengths of zone body and the header.

- Cardholder conditions for erasing — Requests conditions under which cardholder can erase the working zone. As soon as you select this field, a window appears offering the following options:

  - Without protection
  - Either PIN or AID
  - Both PIN and AID

  Select your option using the ↑ and ↓ keys and press RETURN.

- Issuer conditions for erasing: As soon as you select this field, a window appears offering the following options:

  - Without protection
  - Authentication by IK
  - Secure erase by EK
  - Auth. + sec. erase by IK

  Select your option using the ← and → keys and press RETURN.

- Number of the EK/SK for erasing/writing — Asks you for the number of the EK/SK to enable erasing/writing in this zone. Use the ← and → keys to select the value (0, 1, 2, or 3) and then press RETURN.

- Number of the SK for reading — Asks you for the number of the SK to enable reading from this zone. Use the ← and → keys to select the value (0, 1, 2, or 3) and then press RETURN.

- Cardholder conditions for writing — Requests the conditions under which cardholder can write in the working zone. As soon as you select this field, a window appears with the following options:

  - Without protection
  - Either PIN or AID
  - Both PIN and AID

  Select your option using the ↑ and ↓ keys and press RETURN.

- Issuer conditions for writing — Asks you for the conditions required before the application can write in the zone. As soon as you select this field, a window appears with the following options:

  - Without protection
  - Authentication by IK
  - Secure write by SK
  - Auth. + sec. write by IK

  Select your option using the ↑ and ↓ keys and press RETURN.

- Cardholder conditions for reading — Asks you for the conditions to be satisfied before the cardholder can read information in the working zone. As soon as you select this field, a window appears with the following options:

  -
  - Without protection
  - Either PIN or AID
  - Both PIN and AID

  Select your option using the ↑ and ↓ keys and press RETURN.

- Issuer conditions for reading — Asks for the conditions under which the application can read information in this zone. When you select this field, a window appears with the following options:

  - Without protection
  - Authentication by IK or SK
  - Authentication by SK
  - Authentication by IK

  Select your option using the [↑] and [↓] keys and press [RETURN].

NOTE There **are** two options for the same condition — authentication by IK.

- Tracing option — Asks if this option is to be in effect for this working zone. Use the [←] and [→] keys to select between ON and OFF, and then press the [RETURN] key.

- Invalidation lock — Asks if the header being created is invalid. Leave this bit at '1' during the creation phase.

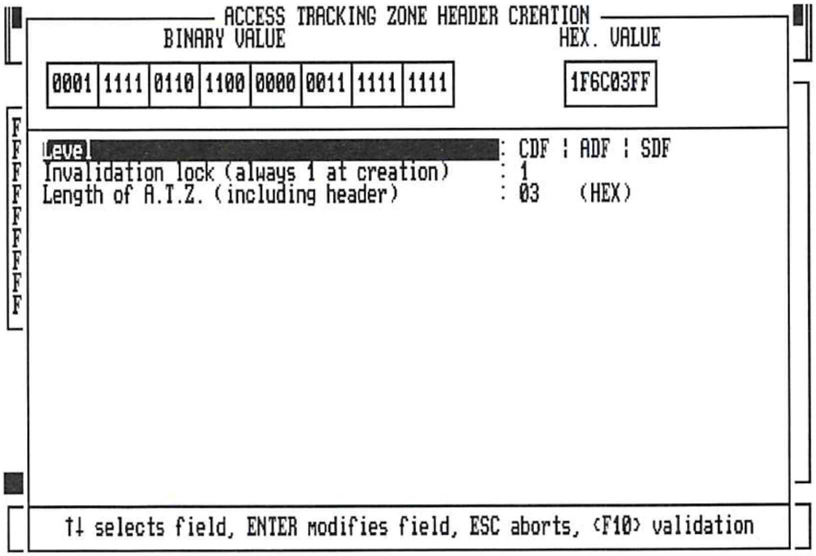
Create ATZ Header

FUNCTION Enables you to create Access Tracking Zone headers.

INVOCATION Select *Create ATZ Header* from the *Power Tools* menu.

After starting the function, the following screen appears:

FIGURE 4-12 CREATE ATZ HEADER



```
               ACCESS TRACKING ZONE HEADER CREATION
            BINARY VALUE                                  HEX. VALUE

 0001 1111 0110 1100 0000 0011 1111 1111                  1F6C03FF

 Level                                      : CDF ¦ ADF ¦ SDF
 Invalidation lock (always 1 at creation)   : 1
 Length of A.T.Z. (including header)        : 03    (HEX)

   ↑↓ selects field, ENTER modifies field, ESC aborts, <F10> validation
```

When all the parameters of the header are set to your satisfaction, press the F10 key to indicate that you have finished designing the header. You are then prompted for the function to use to write the header to the card.

As you select each field, the corresponding part of the binary display in the main menu flashes. As you type in the parameters, the changes are incorporated in this menu.

The control panel comprises three fields:

- Level — Enter the level of the header. Use the ← and → keys to select the level (CDF, ADF or SDF), then press RETURN.

- Invalidation lock — Asks if the header created is invalid. Leave this byte at "1" during the creation phase.

- Length of Access Tracking Zone — Enter the length of the ATZ, enter all figures in hexadecimal.

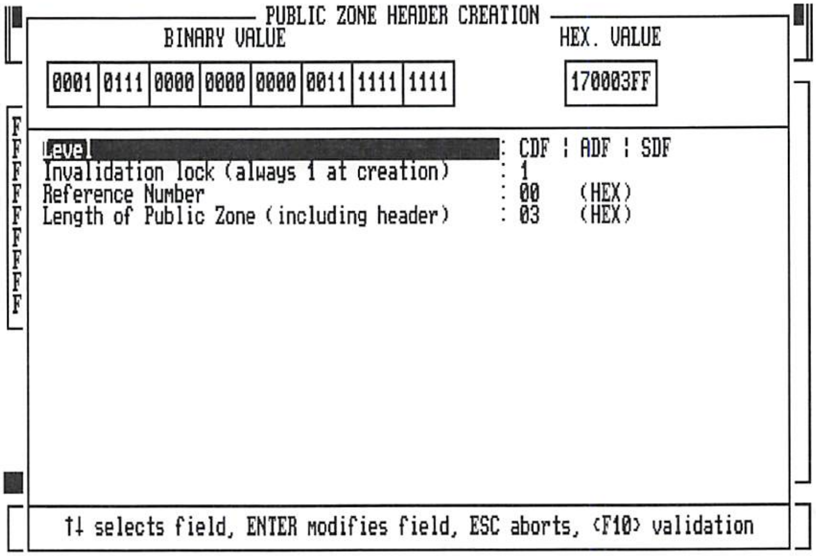
Create Public Zone Header

FUNCTION Enables you to create a header for a public zone.

INVOCATION Select *Create Public Zone Header* from the *Power Tools* menu.

After starting the function, the following screen appears:

FIGURE 4-13 CREATE PUBLIC ZONE HEADER



```
                     PUBLIC ZONE HEADER CREATION
          BINARY VALUE                                   HEX. VALUE
 0001 0111 0000 0000 0000 0011 1111 1111                  170003FF

 Level                                          : CDF ¦ ADF ¦ SDF
 Invalidation lock (always 1 at creation)       : 1
 Reference Number                               : 00    (HEX)
 Length of Public Zone (including header)       : 03    (HEX)

   ↑↓ selects field, ENTER modifies field, ESC aborts, <F10> validation
```

When all the parameters of the header are set to your satisfaction, press the F10 key to indicate that you have finished designing the header. You are then prompted for the function to use to write the header to the card.

As you select each field, the corresponding part of the binary display in the main menu flashes. As you enter the parameters, the changes are incorporated in this menu.

The control panel comprises four fields:

- Level — Enter the level of the header. Use the ← and → keys to select the level (CDF, ADF or SDF), then press RETURN.

- Invalidation lock — Prompt asking if the header being created is invalid. Leave this byte at "1" during the creation phase.

- Reference Number — This is any number between "00" and "FF", composed to allow the App to identify the zone at some later time.

- Length of Public Zone — Prompt asking the length of the PZ: enter all figures in hexadecimal.

Analyse Header Value

FUNCTION Enables you to examine the contents and meaning of a header.

INVOCATION Select *Analyse Header Value* from the *Power Tools* menu.

After starting the function, the following prompt appears:

```
Enter Header Word : ■ ■ ■ ■ ■ ■ ■ ■
```

Enter the hex representation of the header. If it is a DF or a WZ there will be two words to enter. The first will be analysed and, if a second is required, the program will request it:

```
3F0000C8 signifies a 2-word header. Enter second part of the header:■ ■ ■ ■ ■ ■ ■ ■
```

Here we entered a CDF header.

The header is evaluated and presented in the same way as when it was created, using the same screens. The only difference is that the screens are "read-only", and you must use ESC to return to the *Power Tools* menu.

Note that you can use the Grab function to take a header value from the Display window.

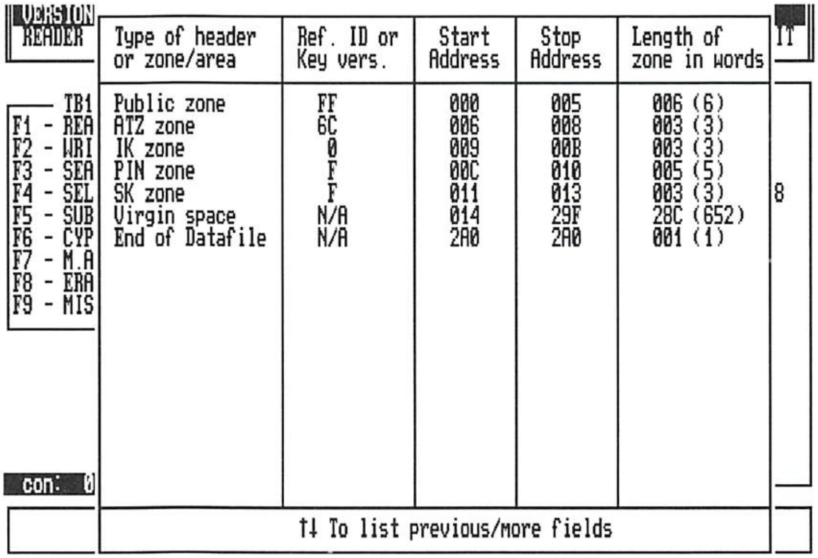
Analyse DF Contents

FUNCTION Enables you to examine the contents and meaning of a Data File.

INVOCATION Select *Analyse DF Contents* from the *Power Tools* menu.

On starting the function, the program interrogates the card — this is visible through a number of "90 00" status results, one for each interrogation. After this phase a screen similar to that shown in Figure 4-14 is presented.

FIGURE 4-14 SAMPLE ANALYSIS OF A DF



Type of header or zone/area	Ref. ID or Key vers.	Start Address	Stop Address	Length of zone in words
Public zone	FF	000	005	006 (6)
ATZ zone	6C	006	008	003 (3)
IK zone	0	009	00B	003 (3)
PIN zone	F	00C	010	005 (5)
SK zone	F	011	013	003 (3)
Virgin space	N/A	014	29F	28C (652)
End of Datafile	N/A	2A0	2A0	001 (1)

↑↓ To list previous/more fields

This screen shows a list of all the structures within the Current DF — although not within any DFs that are themselves within the Current DF. This list is arranged in order of occurrence within the DF. Use the ↑ and ↓ keys to scroll the display, and the ESC key to return to the *Power Tools* menu.

The *DF Analysis* display screen has five columns:

- Type of header or zone/area — This identifies which sort of a structure (if any) has been found. The types supported are:
  - Virgin Space
  - Data File
  - Secret Word
  - Public Zone
  - Working Zone
  - Access Tracking Zone
  - Secret Zone
  - Unknown

  The last entry is always
  - End of Data File

- Ref. ID or Key vers. — This is either the title of the DF or Zone, or else the identifier of the key held within the Secret Zone shown

- Start Address — Start address of the structure relative to the start of the Current DF

- Stop Address — End address of the structure, also relative to the start of the Current DF

- Length of zone in words

NOTE If the Current Data Structure is not a DF, the results from this function are not predictable.

General

The Index menu provides a set of nine general functions available through the keyboard function keys. These are:

F1 - Read — a set of three read functions:

- read data
- list directory
- certify

F2 - Write — a set of eight write functions:

- write data
- create DF or Zone
- write lock FL
- write lock UL
- secure write data by IK
- secure write data by SK
- secure write header by IK
- secure write header by SK

F3 - Search — a set of six search functions. These present the two search instructions provided by the card in a more usable fashion:

- without pattern mask
- first non-virgin word
- forward for equality
- forward for inequality
- backward for equality
- backward for inequality

F4 - Select — a set of four structure selection functions:

- first header
- last header
- next header
- previous header

F5 - Submit Keys — a set of seven key submission functions:

- AK
- PIN
- AID
- IK. Note that this instruction is also used for FK and PK.
- SK
- PIN (cyphered mode)
- AID (cyphered mode)

❖F6 - Cypher Functions — a set of five functions supporting the DEA capabilities of the card.

- load temporary key
- load and diversify temporary key
- diversify temporary key
- ❖ encrypt
- ❖ decrypt

F7 - M.A.C. — three functions to allow generation of M.A.C. values:

- start M.A.C.
- compute M.A.C.
- verify M.A.C.

F8 - Erase — three functions for erasing data from working zones:

- erase data
- secure erase by IK
- secure erase by EK

F9 - Miscellaneous — three other functions not included above:

- read result
- generate random
- invalidation

❖ Restricted functions: see the relevant section for more details.

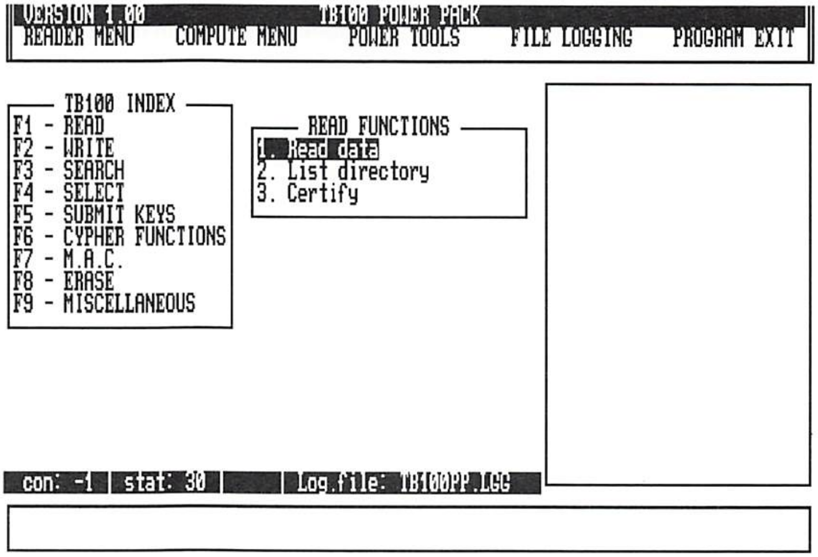
READ FUNCTIONS

General

This section describes the functions used for read operations. A read operation is one of three activities:

- Reading of data
- Listing of headers
- Certifying a value

FIGURE 5-01 READ FUNCTIONS



Having used F1 to get to this menu, there are two ways of selecting the function you wish to use:

- type the number to the left of the function name (from 1 to 3). This will invoke the function immediately.
- use the ↑ and ↓ keys to position the cursor highlight over the desired operation, and then press RETURN.

Read Data

FUNCTION

You use this function to read one or more words on the card.

INVOCATION

Select *Read Data* from the *Read* menu in the *TB100 Index* list.

PARAMETERS

When the function starts, the first prompt appears, giving a default value. This is either zero or one word greater than the last word read with this command.

```
Start address 000 : ■ ■ ■
```

Enter the address (in hexadecimal) of the point where reading is to start. Press RETURN.

The next prompt requests the amount of data you wish to read. The default here is "10", as sixteen words are all that will be visible in the Display window. You can read more, if you wish.

```
Start address xxx   Length 10 : ■ ■ ■
```

Type the number of words to be displayed (in hexadecimal). Then press the RETURN key.

RESPONSE

The words are displayed in the Display window, preceded by the status word.

List Directory

FUNCTION

Displays all the Data File headers and zones in the current Data File.

INVOCATION

Select *List Directory* from the *Read* menu in the *TB100 Index* list.

PARAMETERS

When the function starts, the first prompt appears, giving a default value. This is either zero or one word greater than the last word read with this command.

```
Start address 000 : ■ ■ ■
```

Enter the address (in hexadecimal) of the point where reading is to start. Press RETURN.

The next prompt requests the amount of data you wish to read. The default here is "10", as sixteen words are all that will be visible in the Display window. You can read more, if you wish.

```
Start address xxx   Length 10 : ■ ■ ■
```

Type the number of words to be displayed (in hexadecimal). Then press the RETURN key.

RESPONSE

Gives a list of all the words actually in the Current Data Structure. If this is a Data File, any words in the bodies of child structures will **not** be shown. There is an example of this "trap" at the start of Chapter 3.

Certify

FUNCTION

Generates a certificate value on the card.

INVOCATION

Select *Certify* from the *Read* menu in the *TB100 Index* list.

PARAMETERS

The function starts by requesting the address of the word to be certified:

```
Address 000 : ■ ■ ■
```

The address must be entered in hexadecimal. Next enter the KRP of the AK key to be used for the certification:

```
Key Reference Pattern 0000 : ■ ■ ■ ■
```

Finally, enter the external value for the calculation:

```
External Value : ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■
```

You will now be requested to confirm your entry. Look carefully at the data you have entered.

- If the data is correct, press Y (Yes) to enter the data, you will be returned to the menu.
- If you see a mistake, press N (No). No data is entered and you are returned to the *TB100 Index* menu.

RESPONSE

The card will calculate a certificate which you can now retrieve using the *read result* instruction, also in this same *Read* menu.

NOTE

If you press RETURN during input of the Address and Key Reference Pattern fields the displayed default values will be used.

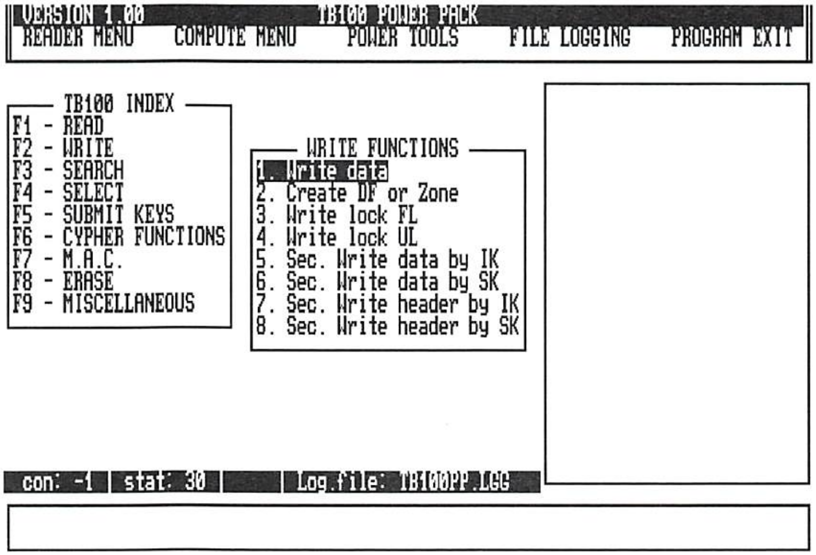
WRITE FUNCTIONS

General

This section describes the functions used for write operations. A write operation is one of the following activities:

- Writing of data
- Creation of a Data File (DF) or a Zone
- Writing of a key
- Writing of data protected by a key
- Writing of headers protected by a key

FIGURE 5-02 WRITE FUNCTIONS MENU



Having used F2 to get to this menu, there are two ways of selecting the function you wish to use:

- type the number to the left of the function name (from 1 to 8). This will invoke the function immediately.
- use the ↑ and ↓ keys to position the cursor highlight over the desired operation, and then press RETURN.

Write Data

FUNCTION

Writes a word to the card EEPROM.

INVOCATION

Select *Write Data* from the *Write* menu in the *TB100 Index* list.

PARAMETERS

Once the function is started, a series of prompts will appear in the data-entry window. The first requests the address in the card EEPROM where the data is to be written:

```
Address 000 : ■■■
```

Enter the address (in hexadecimal). The next prompt asks for the data itself:

```
Data 00000000 : ■■■■■■■■
```

Enter the data word (again in hexadecimal). You will now see a confirmation box. Look carefully at the data you have entered.

- If the data is correct, press Y (Yes) to enter the data. You will be returned to the *TB100 Index* menu.
- If you see a mistake, press N (No). No data is entered and you are returned to the *TB100 Index* menu.

NOTE

Empty input fields are allowed; the default values shown in the prompts will be used instead.

Create DF Or Zone

FUNCTION

Creates a new Data File (DF) or Zone on the card. The function creates the Data Structure header. If the creation is successful, the new DF or Zone is automatically selected as the Current Data Structure.

INVOCATION

Select *Create DF Or Zone* from the *Write* menu in the *TB100 Index* list.

PARAMETERS

When the function starts, a prompt appears in the Data Entry window:

```
Address 000 : ■ ■ ■
```

Type the address (in hexadecimal). The next prompt asks how long the header will be. Data Files and Working Zones have two-word headers, all the other structures use just one word.

```
1-word or 2-words header : ■
```

You are now prompted for the contents (in hexadecimal) of the header. Depending on the size of the header, this will be one of the following two prompt lines:

```
Contents of 1-word header : ■ ■ ■ ■ ■ ■ ■ ■

Contents of 2-word header : ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■
```

You will now see a confirmation box. Look carefully at the data you have entered.

- If the data is correct, press Y (Yes) to enter the data. You will be returned to the *TB100 Index* menu.
- If you see a mistake, press N (No). No data is entered and you are returned to the *TB100 Index* menu.

NOTE

Empty input fields are allowed; the default values shown in the prompts will be used instead.

Write Lock FL

FUNCTION

Sets the Fabrication Lock. When fabrication is finished and the fabrication lock FL is set, the card enters Personalisation Phase.

INVOCATION

Select *Write Lock FL* from the *Write* menu in the *TB100 Index* list.

PARAMETERS

When the function starts, a confirmation prompt appears in the Data Entry window:

```
OK to write FL ?
```

Press Y (Yes) to set the fabrication lock.
Press N (No) to abort the function.

The process of writing the Fabrication Lock is automatic. You are returned to the *TB100 Index* menu.

Write Lock UL

FUNCTION

Writes the Utilisation Lock (UL) of the Current DF. The UL informs the system that the DF is in Utilisation Phase.

INVOCATION

Select *Write Lock UL* from the *Write* menu in the *TB100 Index* list.

PARAMETERS

When the function starts, a confirmation prompt appears in the Data Entry window:

```
OK to write UL ?
```

Press Y (Yes) to set the utilisation lock.

Press N (No) to abort the function.

The process of writing the Utilisation Lock is automatic. You are returned to the *TB100 Index* menu.

Secure Write Data By IK

FUNCTION

Writes data to the card. This data is protected *en route* to the card by encryption with the Issuer Key, IK.

INVOCATION

Select *Secure Write Data By IK* from the *Write* menu in the *TB100 Index* list.

PARAMETERS

When the function starts, you are prompted for the address (in hexadecimal) to write to:

```
Address xxx : ■ ■ ■
```

The address of the current word is displayed as the default value; you need only press RETURN to use it. To use a different address, type the new address and press RETURN. The next prompt is for the data to be given to the function. It is called "Decr. Data" because it is decrypted before transmission to the card, and encrypted by the card to retrieve the original value.

```
Decr. data 00000000 00000000 : ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■
```

After entering the data a confirmation box appears towards the bottom of the screen. Look carefully at the data you have entered.

- If the data is correct, press Y (Yes) to enter the data. You will be returned to the *TB100 Index* menu.
- If you see a mistake, press N (No). No data is entered and you are returned to the *TB100 Index* menu.

Secure Write Data By SK

FUNCTION

Writes data to the card. This data is protected *en route* to the card by encryption with a selected Service Key, SK.

INVOCATION

Select *Secure Write Data By SK* from the *Write* menu in the *TB100 Index* list.

PARAMETERS

When the function starts, you are prompted for the address (in hexadecimal) to write to:

```
Address 000 : ■ ■ ■
```

The address of the current word is displayed as the default value; you need only press RETURN to use it. To use a different address type the new address and press RETURN. The next prompt is for the KRP of the SK to be used. This is required because there may be more than one SK (there is only ever one IK).

```
Key Reference Pattern 0000 : ■ ■ ■ ■
```

Type in the Key Reference Pattern (two bytes, in hexadecimal) and then press RETURN.

The next prompt is for the data to be given to the function. It is called "Decr. Data" because it is decrypted before transmission to the card, and encrypted by the card to retrieve the original value.

```
Decr. data 00000000 00000000 : ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■
```

Enter the decryption data and then press RETURN.

NOTE

If the result of the last encryption operation is displayed on the screen you may use it; press only the RETURN key. To use any other encrypted value, type in the value and then press RETURN.

After entering the data a confirmation box appears towards the bottom of the screen. Look carefully at the data you have entered.

- If the data is correct, press Y (Yes) to enter the data. You will be returned to the *TB100 Index* menu.
- If you see a mistake, press N (No). No data is entered and you are returned to the *TB100 Index* menu.

Secure Write Header By IK

FUNCTION

Writes header data that is protected *en route* to the card by the Issuer Key.

INVOCATION

Select *Secure Write Header by IK* from the *Write* menu in the *TB100 Index* list.

PARAMETERS

When the function starts, the following prompt appears in the Data Entry window:

```
Address 000 : ■ ■ ■
```

Enter the address (in hexadecimal) of the header of the new structure. After you press RETURN the next prompt is displayed:

```
1-word or 2-words header : ■
```

Enter 1 or 2 followed by RETURN. According to the header size, you are now prompted for either one of two words of "decrypted" header data:

```
Decrypted 1-wrd header:■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■

Decrypted 2-wrd header:■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■
```

After entering the data a confirmation box appears towards the bottom of the screen. Look carefully at the data you have entered.

- If the data is correct, press Y (Yes) to enter the data. You will be returned to the *TB100 Index* menu.
- If you see a mistake, press N (No). No data is entered and you are returned to the *TB100 Index* menu.

NOTE

If you use a two word header, you must enter a decrypted value for each word.

Secure Write Header By SK

FUNCTION

Writes header data that is protected *en route* to the card by a Service Key.

INVOCATION

Select *Secure Write Header by SK* from the *Write* menu in the *TB100 Index* list.

PARAMETERS

When the function starts, the following prompt appears in the Data Entry window:

```
Address 000 : ■ ■ ■
```

Enter the address (in hexadecimal) of the header of the new structure. After you press RETURN the next prompt is displayed This is for the Key Reference Pattern (KRP) of the SK to be used. This is required because there may be more than one SK (there is only ever one IK).

```
Key Reference Pattern 0000 : ■ ■ ■ ■
```

Type in the KRP (two bytes, in hexadecimal) and then press RETURN. You will now need to tell the program how long the header is going to be. You will see the prompt:

```
1-word or 2-words header : ■
```

Enter 1 or 2 followed by RETURN. According to the header size, you are now prompted for either one of two words of "decrypted" header data:

```
Decrypted 1-wrd header:■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■

Decrypted 2-wrd header:■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■
```

After entering the data a confirmation box appears towards the bottom of the screen. Look carefully at the data you have entered.

- If the data is correct, press Y (Yes) to enter the data. You will be returned to the *TB100 Index* menu.
- If you see a mistake, press N (No). No data is entered and you are returned to the *TB100 Index* menu.

NOTE

If you use a two word header, you must enter a decrypted value for each word.

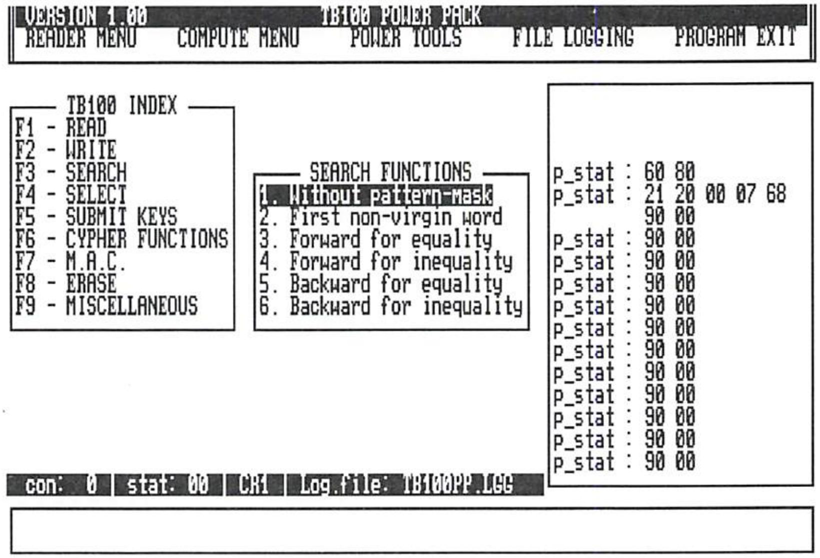
SEARCH FUNCTIONS

General

This section describes the functions that do search operations. Six types of search are available:

- Search without pattern mask
- Search for non-virgin word
- Forward search for equality
- Forward search for inequality
- Backward search for equality
- Backward search for inequality

FIGURE 5-03 SEARCH FUNCTIONS MENU



```
p_stat : 60 80
p_stat : 21 20 00 07 68
         90 00
p_stat : 90 00
p_stat : 90 00
p_stat : 90 00
p_stat : 90 00
p_stat : 90 00
p_stat : 90 00
p_stat : 90 00
p_stat : 90 00
p_stat : 90 00
p_stat : 90 00
p_stat : 90 00
```

Having used F3 to get to this menu, there are two ways of selecting the function you wish to use:

- type the number to the left of the function name (from 1 to 6). This will invoke the function immediately.
- use the ↑ and ↓ keys to position the cursor highlight over the desired operation, and then press RETURN.

NOTE

The contents of Figure 5-03 indicate that the last instruction before invoking the *Search* menu was an *Analyse DF* from the *Power Tools* menu.

Search Without Pattern Mask

FUNCTION

Searches for one- or two-byte patterns in data words in the current zone.

INVOCATION

Select *Without pattern-mask* from the *Search* menu in the *TB100 Index* list.

PARAMETERS

Once the function is started, a series of prompts will appear in the data-entry window. The first requests the address in the card EEPROM from where the search is to start:

```
Start Address 000 : ■ ■ ■
```

Enter the address (in hexadecimal). The next prompt asks for the size of the pattern to be searched for. This can be zero, one, or two bytes (zero implies looking for a virgin word).

```
Number of Arg. bytes : ■
```

Enter the size of the data to search for. You may specify zero, one, or two bytes of data. If you specify zero bytes, the content defaults to a search for a virgin word. If you have specified one or two bytes of data, the next prompt asks for the pattern to be searched for.

```
Argument : ■ ■ ■ ■
```

Enter the data, followed by RETURN. You will now see a confirmation box. Look carefully at the data you have entered.

- If the data is correct, press Y (Yes) to enter the data. You will be returned to the *Search Functions* menu.
- If you see a mistake, press N (No). No data is entered and you are returned to the *Search Functions* menu.

NOTE

Empty input fields are allowed; the default values shown in the prompts will be used instead.

Search For First Non-Virgin Word

FUNCTION Searches for first word with a value different from "FFFFFFFF".

INVOCATION Select *First non-virgin word* from the *Search* menu in the *TB100 Index* list.

PARAMETERS Once the function is started, a series of prompts will appear in the data-entry window. The first requests the address in the card EEPROM from where the search is to start:

```
Start Address 000 : ■ ■ ■
```

Enter the address (in hexadecimal).

To obtain the result, use the read result instruction (Choose the *Search* menu from the *TB100 Index* list).

NOTE Empty input fields are allowed; the default values shown in the prompts will be used instead.

Search Forward For Equality

FUNCTION

You enter a pattern and a mask, and the function searches forward for an identical masked pattern. When the function finds the first identical pattern, it displays it on the screen.

INVOCATION

Select *Forward for equality* from the *Search* menu in the *TB100 Index* list.

PARAMETERS

Once the function is started, a series of prompts will appear in the data-entry window. The first requests the address in the card EEPROM from where the search is to start:

```
Start Address 000 : ■ ■ ■
```

Enter the address (in hexadecimal). The next prompt asks for the pattern to be searched for.

```
Argument : ■ ■ ■ ■ ■ ■ ■ ■
```

Enter the data, followed by RETURN. Your next prompt is for a logical mask for the pattern. For details, see the sections on search instructions in the TB100 Reference Manual.

```
Mask : ■ ■ ■ ■ ■ ■ ■ ■
```

You will now see a confirmation box. Look carefully at the data you have entered.

- If the data is correct, press Y (Yes) to enter the data. You will be returned to the *Search Functions* menu.
- If you see a mistake, press N (No). No data is entered and you are returned to the *Search Functions* menu.

NOTE

Empty input fields are allowed; the default values shown in the prompts will be used instead.

Search Forward For Inequality

FUNCTION

You enter a pattern and a mask, the function then finds the first non-matching masked pattern.

INVOCATION

Select *Forward for inequality* from the *Search* menu in the *TB100 Index* list.

PARAMETERS

Once the function is started, a series of prompts will appear in the data-entry window. The first requests the address in the card EEPROM from where the search is to start:

```
Start Address 000 : ■ ■ ■
```

Enter the address (in hexadecimal). The next prompt asks for the pattern to be searched for.

```
Argument : ■ ■ ■ ■ ■ ■ ■ ■
```

Enter the data, followed by RETURN. Your next prompt is for a logical mask for the pattern. For details, see the sections on search instructions in the TB100 Reference Manual.

```
Mask : ■ ■ ■ ■ ■ ■ ■ ■
```

You will now see a confirmation box. Look carefully at the data you have entered.

- If the data is correct, press Y (Yes) to enter the data. You will be returned to the *Search Functions* menu.
- If you see a mistake, press N (No). No data is entered and you are returned to the *Search Functions* menu.

NOTE

Empty input fields are allowed; the default values shown in the prompts will be used instead.

Search Backward For Equality

FUNCTION

Search backward for the first matching masked pattern.

INVOCATION

Select *Backward for equality* from the *Search* menu in the *TB100 Index* list.

PARAMETERS

Once the function is started, a series of prompts will appear in the data-entry window. The first requests the address in the card EEPROM from where the search is to start. The highest possible address is "29E".

```
Start Address 000 : ■ ■ ■
```

Enter the address (in hexadecimal). The next prompt asks for the pattern to be searched for.

```
Argument : ■ ■ ■ ■ ■ ■ ■ ■
```

Enter the data, followed by RETURN. Your next prompt is for a logical mask for the pattern. For details, see the sections on search instructions in the TB100 Reference Manual.

```
Mask : ■ ■ ■ ■ ■ ■ ■ ■
```

You will now see a confirmation box. Look carefully at the data you have entered.

- If the data is correct, press Y (Yes) to enter the data. You will be returned to the *Search Functions* menu.
- If you see a mistake, press N (No). No data is entered and you are returned to the *Search Functions* menu.

NOTE

Empty input fields are allowed; the default values shown in the prompts will be used instead.

Search Backward For Inequality

FUNCTION

Search backward for the first non-matching masked pattern.

INVOCATION

Select *Backward for inequality* from the *Search* menu in the *TB100 Index* list.

PARAMETERS

Once the function is started, a series of prompts will appear in the data-entry window. The first requests the address in the card EEPROM from where the search is to start. The highest possible address is "29E".

```
Start Address 000 : ■ ■ ■
```

Enter the address (in hexadecimal). The next prompt asks for the pattern to be searched for.

```
Argument : ■ ■ ■ ■ ■ ■ ■ ■
```

Enter the data, followed by RETURN. Your next prompt is for a logical mask for the pattern. For details, see the sections on search instructions in the TB100 Reference Manual.

```
Mask : ■ ■ ■ ■ ■ ■ ■ ■
```

You will now see a confirmation box. Look carefully at the data you have entered.

- If the data is correct, press Y (Yes) to enter the data. You will be returned to the *Search Functions* menu.
- If you see a mistake, press N (No). No data is entered and you are returned to the *Search Functions* menu.

NOTE

Empty input fields are allowed; the default values shown in the prompts will be used instead.

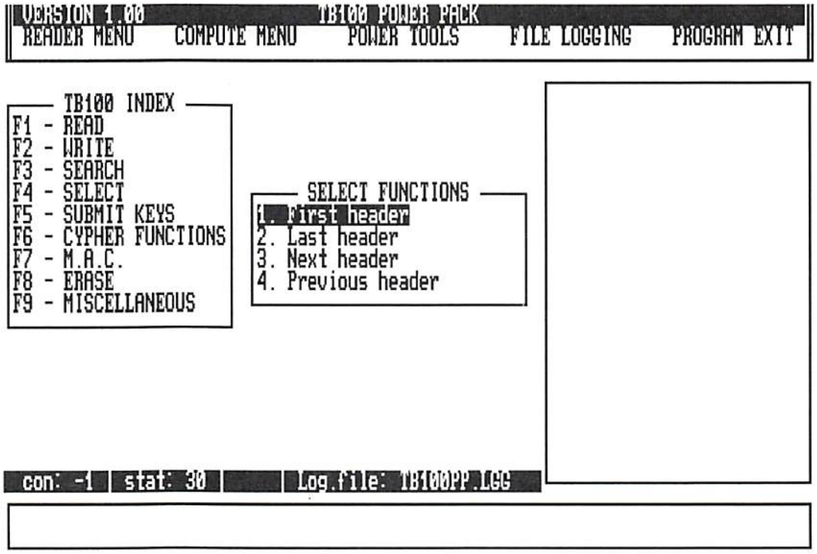
SELECT FUNCTIONS

General

This section describes the functions available for selection operations. Selection operations are used to find the header of your choice. The following are available:

- Selection of the first header of a certain specified type within a Data File (*First header*)
- Selection of the last header of a certain specified type within a Data File (*Last header*)
- Selection of the header of the current type immediately after the current header, and within the same Data File (*Next header*)
- Selection of the header of the current type immediately before the current header, and within the same Data File (*Previous header*)

FIGURE 5-04 SELECT FUNCTIONS MENU



```
VERSION 1.00                    TB100 POWER PACK
READER MENU   COMPUTE MENU   POWER TOOLS   FILE LOGGING   PROGRAM EXIT

 TB100 INDEX
F1 - READ
F2 - WRITE
F3 - SEARCH
F4 - SELECT               SELECT FUNCTIONS
F5 - SUBMIT KEYS        1. First header
F6 - CYPHER FUNCTIONS   2. Last header
F7 - M.A.C.             3. Next header
F8 - ERASE              4. Previous header
F9 - MISCELLANEOUS

 con: -1 | stat: 30 |     | Log.file: TB100PP.LGG
```

Having used F4 to get to this menu, there are two ways of selecting the function you wish to use:

- type the number to the left of the function name (from 1 to 4). This will invoke the function immediately.
- use the ↑ and ↓ keys to position the cursor highlight over the desired operation, and then press RETURN.

Select First Header

FUNCTION

Selects the first header of a Data File or a Zone in the Current Data File.

INVOCATION

Select *First header* from the *Search* menu in the *TB100 Index* list.

PARAMETERS

Once the function is started, a series of prompts will appear in the data-entry window. The first requests the size of the identification pattern to be used to find the header. This may be one or two bytes; the first is essential, and the second holds the HRI data.

```
1-byte or 2-byte pattern : ■
```

Enter either 1 or 2. You will be prompted immediately for the content of the pattern:

```
Pattern : ■ ■ ■ ■
```

The DF is now searched. If such a header exists, it will be selected, and its contents may be retrieved with the *read result* instruction (Select *Read result* from the *Miscellaneous* menu in the *TB100 Index* list). If not, you will see a red warning message, and you must try again.

Select Last Header

FUNCTION Selects the last header of a Data File or a Zone in the Current Data File.

INVOCATION Select *Last header* from the *Search* menu in the *TB100 Index* list.

PARAMETERS Once the function is started, a series of prompts will appear in the data-entry window. The first requests the size of the identification pattern to be used to find the header. This may be one or two bytes; the first is essential, and the second holds the HRI data.

```
1-byte or 2-byte pattern : ■
```

Enter either $\boxed{1}$ or $\boxed{2}$. You will be prompted immediately for the content of the pattern:

```
Pattern : ■ ■ ■ ■
```

The DF is now searched. If such a header exists, it will be selected, and its contents may be retrieved with the *read result* instruction (Select *Read result* from the *Miscellaneous* menu in the *TB100 Index* list). If not, you will see a red warning message, and you must try again.

Select Next Header

FUNCTION Selects the next header in memory (i.e. with a greater address) after the last one you selected. The header will be of the same sort as is currently selected.

INVOCATION Select *Next header* from the *Search* menu in the *TB100 Index* list.

PARAMETERS This function is automatic, all you have to do is start it and then reply to the confirmation box.

Select Previous Header

FUNCTION Selects the previous header in memory (i.e. with a lower address) before the last one you selected. The header will be of the same sort as is currently selected.

INVOCATION Select *Previous header* from the *Search* menu in the *TB100 Index* list.

PARAMETERS This function is automatic, all you have to do is start it and then reply to the confirmation box.

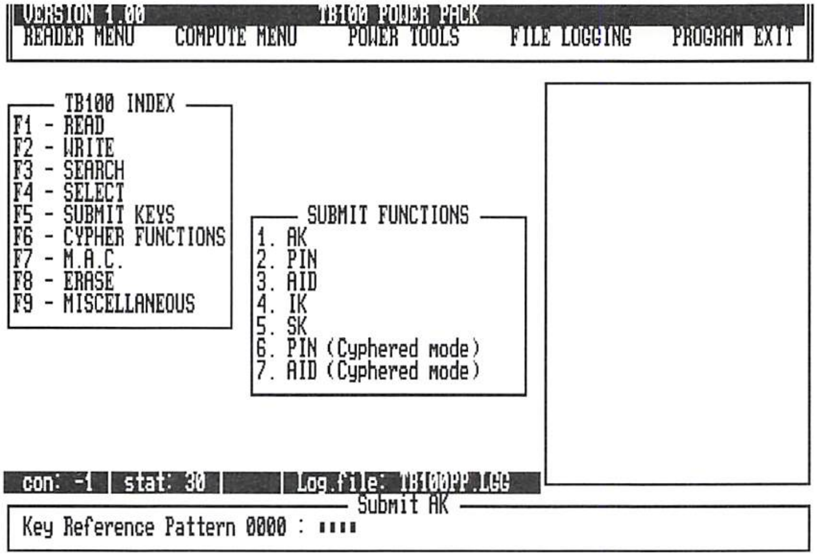
SUBMIT KEYS FUNCTIONS

General

This section describes the functions which enable you to set various keys on the card. They are:

- The Authentication Key — AK
- The Personal Identification Number — PIN
- The Alternate Identification Codes — AID
- The Issuer Key — IK
- The Service Keys — SK

FIGURE 5-05 SUBMIT KEYS MENU



```
con: -1 | stat: 30 |  | Log.file: TB100PP.LGG
Submit AK
Key Reference Pattern 0000 : ▮▮▮▮
```

Having used F5 to get to this menu, there are two ways of selecting the function you wish to use:

- type the number to the left of the function name (from 1 to 7). This will invoke the function immediately.
- use the ↑ and ↓ keys to position the cursor highlight over the desired operation, and then press RETURN.

Key Submission

There are three forms of key submission, depending on the key and the form of submission:

- Issuer Key Submission — where the key is submitted indirectly, via its effect on a random number by the decryption process
- Bearer Key Submission — where the key is submitted directly to the card with no protection whatsoever
- Encrypted Bearer Key Submission — where the key is transformed before submission

The next two sections describe the algorithms used for the first and third cases.

Issuer Key Submission

With these keys — the IK, AK, EK, and SK keys, the algorithm is as follows:

- issue a *generate random* instruction. This generates and loads a pseudo-random number into a buffer in the card RAM. The number is returned to the App.
- issue a *decrypt* instruction, with the random number received from the card as the number to be decrypted and the key involved ("XK") as the decryption key.
- issue a *submit XK* instruction with the result of the decryption. This will be encrypted by the card with the card's version of the keys used, and the card should regain the original random number.

Encrypted Bearer Key Submission

With these keys — the PIN and AID keys, the algorithm is as follows:

- issue a *generate random* instruction. This generates and loads a pseudo-random number into a buffer in the card RAM. The number is returned to the App.
- perform an XOR computation (available as a Power Pack function), with the random number received from the card and the key involved (PIN or AID).
- issue a *decrypt* instruction, with the result of the XOR computation and the authentication key AK of the card.
- issue a *submit key* instruction with the result of the decryption. This will be reconverted by the card and the result will be compared with the original random number.

In either case, loss of the random number in the card for any reason means that you must start the process over again.

Submit AK

FUNCTION

Sends the Authentication Key (AK) to the card.

INVOCATION

Select *Submit AK* from the *Submit keys* menu in the *TB100 Index* list.

PARAMETERS

Once the function is started, a series of prompts will appear in the data-entry window. The first requests the KRP identifier of the key that is to be submitted:

```
Key Reference Pattern 0000 : ■ ■ ■ ■
```

Enter the KRP (in hexadecimal). The next prompt requests the input data (see the beginning of this chapter); enter this (also in hexadecimal),

```
Decr. data 00000000 00000000 : ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■
```

and press RETURN. You will now see a confirmation box. Look carefully at the data you have entered.

- If the data is correct, press Y (Yes) to enter the data. You will be returned to the *Submit Keys* menu.
- If you see a mistake, press N (No). No data is entered and you are returned to the *Submit Keys* menu.

NOTES

Empty input fields are allowed; the default values shown in the prompts will be used instead.

The card does not record this operation, so no jamming occurs if you enter an incorrect Authentication Key.

Submit PIN (Clear Mode)

FUNCTION

Sends the Personal Identification Number (PIN) to the card.

INVOCATION

Select *Submit PIN* from the *Submit keys* menu in the *TB100 Index* list.

PARAMETERS

Once the function is started you are prompted for the PIN value. This is as it will be found in the PIN Secret Zone in the card.

```
PIN 00000000 00000000 : ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■
```

Enter the PIN and press RETURN. You will now see a confirmation box. Look carefully at the data you have entered.

- If the data is correct, press Y (Yes) to enter the data. You will be returned to the *Submit Keys* menu.
- If you see a mistake, press N (No). No data is entered and you are returned to the *Submit Keys* menu.

NOTES

Empty input fields are allowed; the default values shown in the prompts will be used instead.

The *Grab* function can be used to get the PIN value from the Display window.

Submit AID (Clear Mode)

FUNCTION

Sends the Alternate Identification Code (AID) to the card.

INVOCATION

Select *Submit AID* from the *Submit keys* menu in the *TB100 Index* list.

PARAMETERS

Once the function is started you are prompted for the AID value. This is as it will be found in the AID Secret Zone in the card.

```
AID 00000000 00000000 : ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■
```

Enter the PIN and press RETURN. You will now see a confirmation box. Look carefully at the data you have entered.

- If the data is correct, press Y (Yes) to enter the data. You will be returned to the *Submit Keys* menu.
- If you see a mistake, press N (No). No data is entered and you are returned to the *Submit Keys* menu.

NOTES

Empty input fields are allowed; the default values shown in the prompts will be used instead.

The *Grab* function can be used to get the AID value from the Display window.

Submit IK

FUNCTION

Sends the Issuer Key (IK) to the card. The value entered must be encoded.

INVOCATION

Select *Submit IK* from the *Submit keys* menu in the *TB100 Index* list.

PARAMETERS

Once the function is started, you are prompted for the decrypted random number (see the beginning of this chapter); enter this (in hexadecimal),

```
Decr. data 00000000 00000000 : ■■■■■■■■■■■■■■■■
```

and press RETURN. You will now see a confirmation box. Look carefully at the data you have entered.

- If the data is correct, press Y (Yes) to enter the data. You will be returned to the *Submit Keys* menu.
- If you see a mistake, press N (No). No data is entered and you are returned to the *Submit Keys* menu.

NOTE

Empty input fields are allowed; the default values shown in the prompts will be used instead.

Submit SK

FUNCTION

Sends a Service Key (SK) to the card. The value entered must be encoded.

INVOCATION

Select *Submit SK* from the *Submit keys* menu in the *TB100 Index* list.

PARAMETERS

Once the function is started, a series of prompts will appear in the data-entry window. The first requests the KRP identifier of the key that is to be submitted:

```
Key Reference Pattern 0000 : ■ ■ ■ ■
```

Enter the KRP (in hexadecimal). The next prompt requests the decrypted key value (see the beginning of this chapter); enter this (also in hexadecimal),

```
Decr. data 00000000 00000000 : ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■
```

and press RETURN. You will now see a confirmation box. Look carefully at the data you have entered.

- If the data is correct, press Y (Yes) to enter the data. You will be returned to the *Submit Keys* menu.
- If you see a mistake, press N (No). No data is entered and you are returned to the *Submit Keys* menu.

NOTE

Empty input fields are allowed; the default values shown in the prompts will be used instead. If the result of the last decryption operation is shown in the Display window, this can be used (with the *Grab* function).

Submit PIN (Ciphered Mode)

FUNCTION

Sends an enciphered PIN to the card.

INVOCATION

Select *Submit PIN (ciphered mode)* from the *Submit keys* menu in the *TB100 Index* list.

PARAMETERS

Once the function is started, a series of prompts will appear in the data-entry window. The first requests the KRP identifier of the key that is to be submitted:

```
Key Reference Pattern 0000 : ■■■■
```

Enter the KRP (in hexadecimal). The next prompt requests the input data for the function (see the beginning of this chapter); enter this (also in hexadecimal),

```
Decr. data 00000000 00000000 : ■■■■■■■■■■■■■■■■
```

and press RETURN. You will now see a confirmation box. Look carefully at the data you have entered.

- If the data is correct, press Y (Yes) to enter the data. You will be returned to the *Submit Keys* menu.
- If you see a mistake, press N (No). No data is entered and you are returned to the *Submit Keys* menu.

NOTE

Empty input fields are allowed; the default values shown in the prompts will be used instead.

Submit AID (Ciphered Mode)

FUNCTION: Sends the AID (in ciphered mode) to the card.

INVOCATION Select *Submit AID (ciphered mode)* from the *Submit keys* menu in the *TB100 Index* list.

PARAMETERS Once the function is started, a series of prompts will appear in the data-entry window. The first requests the KRP identifier of the AK that is to be used:

```
Key Reference Pattern 0000 : ■ ■ ■ ■
```

Enter the KRP (in hexadecimal). The next prompt requests the data to be submitted (see the beginning of this chapter); enter this (also in hexadecimal),

```
Decr. data 00000000 00000000 : ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■
```

and press RETURN. You will now see a confirmation box. Look carefully at the data you have entered.

- If the data is correct, press Y (Yes) to enter the data. You will be returned to the *Submit Keys* menu.
- If you see a mistake, press N (No). No data is entered and you are returned to the *Submit Keys* menu.

NOTE Empty input fields are allowed; the default values shown in the prompts will be used instead.

CIPHER FUNCTIONS

General

❖ This section describes the functions for ciphering operations. The two
❖ cryptographic functions described may or may not be available on your
❖ card. Availability of these two functions depends on permission from the
❖ appropriate legal authorities. Those sections marked with a "❖" are affected.

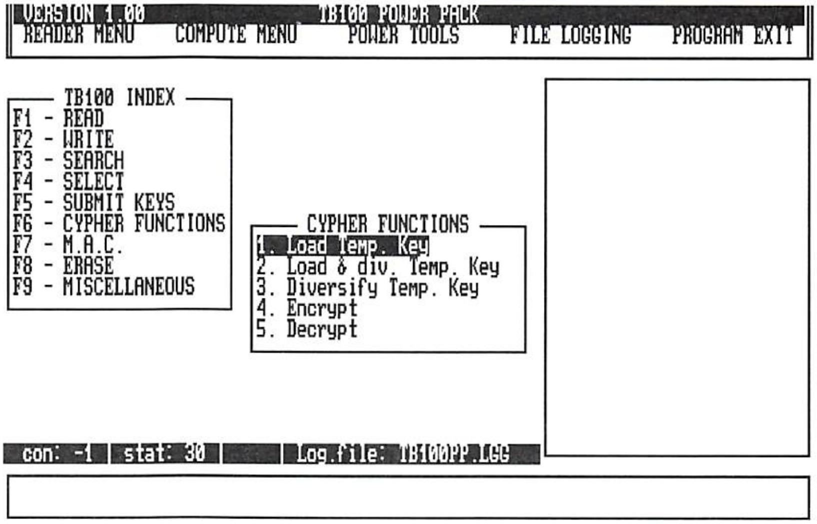
These ciphering functions are:

- operations on temporary keys:
  - loading into RAM
  - loading into RAM and then diversifying

  -diversifying a key that has already been loaded into RAM

❖ - cryptographic functions:
❖   - encryption
❖   - decryption

FIGURE 5-06 CIPHER FUNCTIONS MENU



Having used F6 to get to this menu, there are two ways of selecting the function you wish to use:

- type the number to the left of the function name (from 1 to 5). This will invoke the function immediately.
- use the ↑ and ↓ keys to position the cursor highlight over the desired operation, and then press RETURN.

Load Temporary Key

FUNCTION Generates a temporary key in the card working RAM.

INVOCATION Select *Load Temp. Key* from the *Cypher Functions* menu in the *TB100 Index* list.

PARAMETERS You are prompted for the KRP identifier of the key that is to be loaded:

```
Key Reference Pattern 0000 : ■■■■
```

Enter the KRP (in hexadecimal). You are returned to the *Cypher Functions* menu.

Load and Diversify Temporary Key

FUNCTION

Loads and diversifies the temporary key.

INVOCATION

Select *Load & div. Temp. Key* from the *Cypher Functions* menu in the *TB100 Index* list.

PARAMETERS

You are prompted for the KRP identifier of the key that is to be loaded:

```
Key Reference Pattern 0000 : ■■■■
```

Enter the KRP (in hexadecimal). Next, you must enter the external value to be used for the diversification operation:

```
External value : ■■■■■■■■■■■■■■■■
```

You will now see a confirmation box. Look carefully at the data you have entered.

- If the data is correct, press Y (Yes) to perform the operation. You will be returned to the *Cypher Functions* menu.
- If you see a mistake, press N (No). No operation is performed and you are returned directly to the *Cypher Functions* menu.

Diversify Temporary Key

FUNCTION

Diversifies a temporary key already loaded into the card working RAM.

INVOCATION

Select *Diversify Temp. Key* from the *Cypher Functions* menu in the *TB100 Index* list.

PARAMETERS

When the function is started, a prompt appears in the data-entry window:

```
External or Internal Random Value : ■
```

Select the origin of the value used for diversifying, Press [I] for an internal value, or [E] for an external one.

EXTERNAL VALUES

If you select "E", the following a prompt is displayed:

```
External Random Value : ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■
```

Enter the external value (in hexadecimal), and press [RETURN]. You will now see a confirmation box. Look carefully at the data you have entered.

- If the data is correct, press [Y] (Yes) to perform the operation. You will be returned to the *Cypher Functions* menu.
- If you see a mistake, press [N] (No). No operation is performed and you are returned directly to the *Cypher Functions* menu.

INTERNAL VALUES

If you select "I" the following prompt appears:

```
Internal Random Value : ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■
```

You will now see a confirmation box. Look carefully at the data you have entered.

- If the data is correct, press [Y] (Yes) to perform the operation. You will be returned to the *Cypher Functions* menu.
- If you see a mistake, press [N] (No). No operation is performed and you are returned directly to the *Cypher Functions* menu.

Encrypt

FUNCTION Encrypts an eight-byte value.

INVOCATION Select *Encrypt* from the *Cypher Functions* menu in the *TB100 Index* list.

PARAMETERS: When the function is active, a prompt appears in the data-entry window:

```
Enter data to be encrypted : ■■■■■■■■■■■■■■■■
```

Enter the data value (in hexadecimal), and press RETURN. You will now see a confirmation box. Look carefully at the data you have entered.

- If the data is correct, press Y (Yes) to perform the operation. You will be returned to the *Cypher Functions* menu.
- If you see a mistake, press N (No). No operation is performed and you are returned directly to the *Cypher Functions* menu.

❖ Decrypt

FUNCTION Decrypts an eight-byte value.

INVOCATION Select *Decrypt* from the *Cypher Functions* menu in the *TB100 Index* list.

PARAMETERS: When the function is started, a prompt appears in the data-entry window:

```
Enter data to be decrypted : ■■■■■■■■■■■■■■■■
```

Enter the data value (in hexadecimal), and press RETURN. You will now see a confirmation box. Look carefully at the data you have entered.

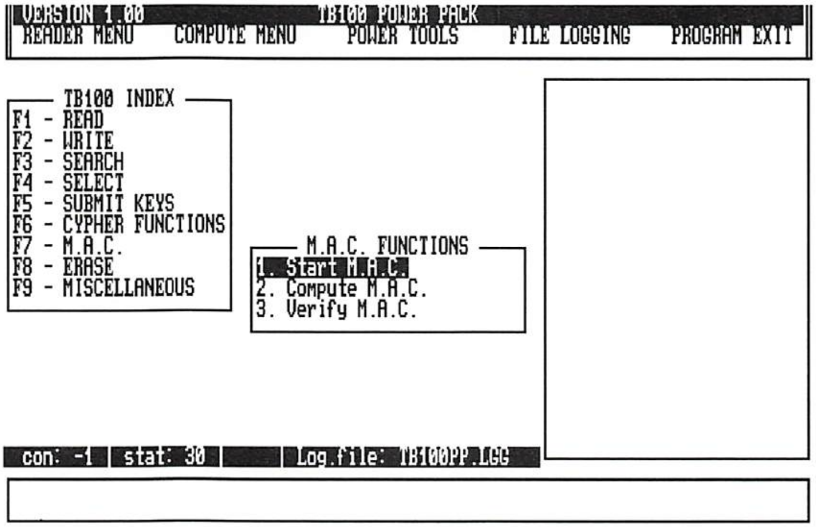
- If the data is correct, press Y (Yes) to perform the operation. You will be returned to the *Cypher Functions* menu.
- If you see a mistake, press N (No). No operation is performed and you are returned directly to the *Cypher Functions* menu.

MAC FUNCTIONS

General

This section describes the functions related to operations for generating and verifying MAC values.

FIGURE 5-07 MAC FUNCTIONS MENU



con: -1 stat: 30 Log.file: TB100PP.LGG

Having used F7 to get to this menu, there are two ways of selecting the function you wish to use:

- type the number to the left of the function name (from 1 to 3). This will invoke the function immediately.
- use the ↑ and ↓ keys to position the cursor highlight over the desired operation, and then press RETURN.

Start MAC

FUNCTION

Starts the process of generating a MAC.

INVOCATION

Select *Start M.A.C.* from the *M.A.C. Functions* menu in the *TB100 Index* list.

PARAMETERS

Once the function is started, a series of prompts will appear in the data-entry window. The first requests the type of start value to be used:

```
External or Internal Start Value : ■
```

You can choose either an External value (type E), or an Internal value (type I).

EXTERNAL VALUE

If you select "E" (External), the following prompt is displayed:

```
External value : ■■■■■■■■■■■■■■■■
```

Enter the full 8-byte (64-bit) value (in hexadecimal) and press RETURN. You will now see a confirmation box. Look carefully at the data you have entered.

- If the data is correct, press Y (Yes) to execute the *start MAC* instruction. You will then be returned to the *M.A.C. Functions* menu.
- If you see a mistake, press N (No). No instruction is executed and you are returned directly to the *M.A.C. Functions* menu.

INTERNAL VALUE

If you select "I" (Internal), the following prompt is displayed:

```
Internal value OK (Y/N)
```

and you respond accordingly.

In either case, an affirmative answer will result in the start MAC function being invoked, while a negative one returns you directly to the *M.A.C. Function* menu again.

Compute MAC

FUNCTION

This function calculates one iteration of the MAC computation.

INVOCATION

Select *Compute M.A.C.* from the *M.A.C. Functions* menu in the *TB100 Index* list.

PARAMETERS

When the function starts, a prompt appears in the Data Entry window:

```
External value : ■■■■■■■■■■■■■■■■
```

Enter the full 8-byte (64-bit) value (in hexadecimal) and press RETURN. You will now see a confirmation box. Look carefully at the data you have entered.

- If the data is correct, press Y (Yes) to execute the instruction. You will then be returned to the *M.A.C. Functions* menu.
- If you see a mistake, press N (No). You will be returned directly to the *M.A.C. Functions* menu.

NOTES

Use the *read result* (see the *Miscellaneous* option in the *TB100 Index* menu) to get the MAC result.

Do not do this until you have executed *compute MAC* enough times. If the required number of executions is fifteen, for example, you must execute one *start MAC* and at least fourteen *compute MAC* instructions before the correct MAC is generated.

Verify MAC

FUNCTION Sends a MAC value entered by the user to the card for verification. The MAC calculated by the card is compared with that presented by the user.

INVOCATION Select *Verify M.A.C.* from the *M.A.C. Functions* menu in the *TB100 Index* list.

PARAMETERS When the function starts, a prompt appears in the data-entry window:

```
Verify value 00000000 00000000 : ■■■■■■■■■■■■■■■■
```

Enter the external value in hexadecimal, and press RETURN.

NOTE If the MAC is verified correctly, the status word will have a value of "90 00."

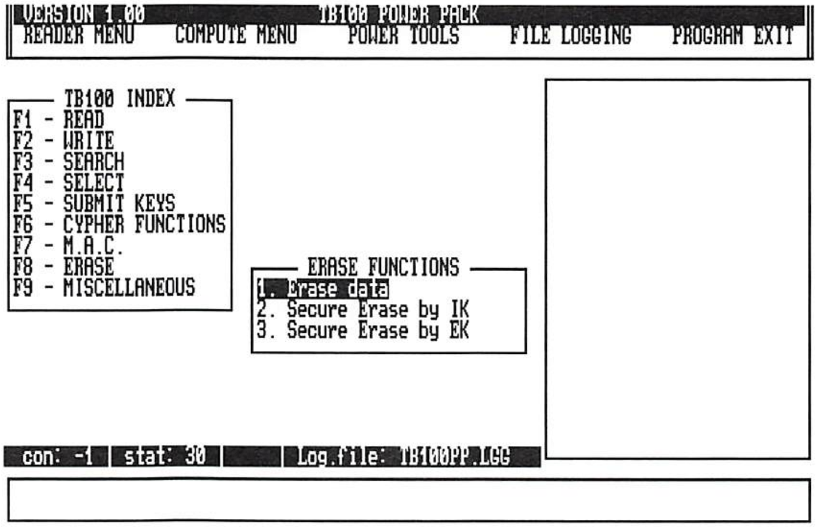
ERASURE OPERATIONS

General

This section describes the functions for erasure operations. These are:

- erasing of data
- erasing of data protected by keys

FIGURE 5-08 ERASE FUNCTIONS MENU



Having used F8 to get to this menu, there are two ways of selecting the function you wish to use:

- type the number to the left of the function name (from 1 to 3). This will invoke the function immediately.
- use the ↑ and ↓ keys to position the cursor highlight over the desired operation, and then press RETURN.

Erase Data

FUNCTION

Erases selected data in the Working Zone of the Data File (DF), or Common Data File (CDF).

INVOCATION

Select *Erase data* from the *Erase Functions* menu in the *TB100 Index* list.

PARAMETERS

Once the function is started, a series of prompts will appear in the data-entry window. The first requests the address of the first word whose contents **are to be** erased:

```
Start address 000 : ■ ■ ■
```

The Current Data Structure must be a Working Zone, and the address must be within the body of the zone. Next, you are prompted for the end address. This is the first address **after the end of** the area to be erased.

```
Start address xxx   End address xxy : ■ ■ ■
```

where the default address `xxy` is always one greater than `xxx`.

You will now see a confirmation box. Look carefully at the data you have entered.

- If the data is correct, press Y (Yes) to enter the data. You will be returned to the *Erase Functions* menu.
- If you see a mistake, press N (No). No data is entered and you are returned to the *Erase Functions* menu.

Secure Erase by IK

FUNCTION

Erases data in the Working Zone. You must have submitted IK **before** you start this function.

INVOCATION

Select *Erase data by IK* from the *Erase Functions* menu in the *TB100 Index* list.

PARAMETERS

Once the function is started, a series of prompts will appear in the data-entry window. The first requests the address of the first word whose contents **are to be** erased:

```
Start address 000 : ■ ■ ■
```

You are now requested for the decrypted data to be sent to the card. This data includes the identifier of the Current Working Zone, the start address, and the end address of the area to be erased, as defined in the erase data instruction above. See the TB100 Reference Manual for information about the precesi composition of this value.

```
Dec. data 00000000 00000000 : ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■
```

You will now see a confirmation box. Look carefully at the data you have entered.

- If the data is correct, press Y (Yes) to enter the data. You will be returned to the *Erase Functions* menu.
- If you see a mistake, press N (No). No data is entered and you are returned to the *Erase Functions* menu.

Secure Erase by EK

FUNCTION: Erases data in the Working Zone, after the authentication of the sender of the instruction.

INVOCATION Select *Erase data by EK* from the *Erase Functions* menu in the *TB100 Index* list.

PARAMETERS Once the function is started, a series of prompts will appear in the data-entry window. The first requests the address of the first word whose contents **are to be** erased:

```
Start address 000 : ■ ■ ■
```

As there may be a number of SK keys in the same Control System, you must now specify which SK is to be used for the secure operation. This is done by providing the KRP of the Secret Zone holding the key:

```
Key Reference Pattern 0000 : ■ ■ ■ ■
```

Next, you are requested for the decrypted data to be sent to the card. This data includes the identifier of the Current Working Zone, the start address, and the end address of the area to be erased, as defined in the erase data instruction above. See the TB100 Reference Manual for information about the precise composition of this value.

```
Dec. data 00000000 00000000 : ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■
```

You will now see a confirmation box. Look carefully at the data you have entered.

- If the data is correct, press Y (Yes) to enter the data. You will be returned to the *Erase Functions* menu.
- If you see a mistake, press N (No). No data is entered and you are returned to the *Erase Functions* menu.

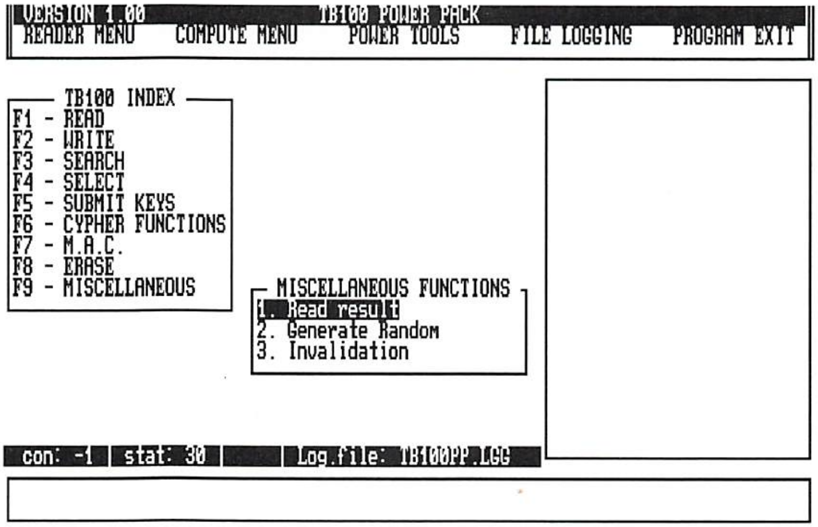
MISCELLANEOUS FUNCTIONS

General

This section describes the functions for various operations such as:

- Reading a result
- Generating a random number
- The invalidation command

FIGURE 5-09 MISCELLANEOUS FUNCTIONS MENU



Having used F9 to get to this menu, there are two ways of selecting the function you wish to use:

- type the number to the left of the function name (from 1 to 3). This will invoke the function immediately.
- use the ↑ and ↓ keys to position the cursor highlight over the desired operation, and then press RETURN.

Read Result

FUNCTION Reads the result generated by the last instruction.

INVOCATION Select *Read result* from the *Miscellaneous Functions* menu in the *TB100 Index* list.

PARAMETERS Once the function is started the following prompt will appear in the data-entry window:

```
Select result length -> 08 0C 14
```

One of the three options is illuminated in reverse-video. select the option you desire using the ← and → keys and press RETURN.

- "08" — *search* functions
- "08" — *cipher* functions
- "08" — *MAC* functions
- "0C" — *select* functions (except below)
- "14" — *select* MAC Secret Zone

The data will be shown in the Display window to the right of the screen.

Generate Random Number

FUNCTION

Makes the card generate a random number.

INVOCATION

Select *Generate Random* from the *Miscellaneous Functions* menu in the *TB100 Index* list.

PARAMETERS

When the function starts, the random number generated by the card appears automatically in the Display window, preceded by the legend "*Rnd*". It may be copied from here using the *Grab* function.

No data entry is necessary with this function.

Invalidation

FUNCTION

Prevents further use of a Data File or Zone, making it move between the Utilisation and End-Of-Life Phases. A form of the *submit IK* instruction is used.

INVOCATION

Select *Invalidation* from the *Miscellaneous Functions* menu in the *TB100 Index* list.

PARAMETERS

When the function starts, a prompt for a number appears in the data-entry window. This value is composed as follows:

generate random
complement it
decrypt with IK as the key

```
Decr. Data 00000000 00000000 : ■■■■■■■■■■■■■■■■
```

Enter the encrypted value, and press RETURN.

You will now see a confirmation box. Look carefully at the data you have entered.

- If the data is correct, press Y (Yes) to invalidate the structure. You will be returned to the *Miscellaneous Functions* menu.
- If you see a mistake, press N (No). No function is executed and you are returned to the *Miscellaneous Functions* menu.

APPENDIX A THE HELP AND LOG FILES

The Help File

As explained in Chapter 2, the Help function of the Power Pack is implemented via a file — *TB100PP.HLP* — holding the help text. This Help file can be translated or modified, by adding personal notes etc.

The file is written in ASCII format and has the name *TB100PP.HLP*. You can edit it with any ASCII editor. Remember to make a copy of the file before you modify it.

The Help file is made up of blocks, each one corresponding to an instruction. Each block contains a header and a body with up to 1999 lines of text. Blocks are separated by a page-feed symbol (ASCII 12).

NOTE If your keyboard does not have the page-feed symbol, type *12* on the PC numeric keypad while holding the ALT key depressed. When the ALT key is then released the symbol for a page-feed will appear.

BLOCK Each block is composed of a number of text lines, of which the first is reserved as the header and the last must hold only a pagefeed symbol. In between you may have up to 1999 lines of body text.

NOTE Each block corresponds to an instruction, so the order of blocks must be identical to that of the original file.

FIGURE A-01 A FRAGMENT OF A HELP FILE

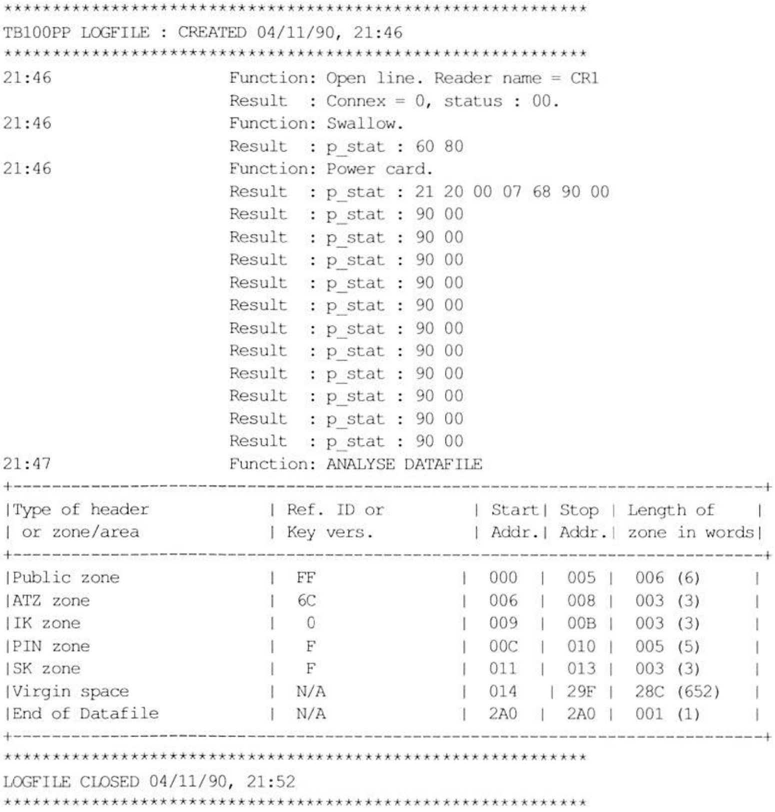
```
HELP ON HELP
Within TB100PP you can ask for on-line help by pressing ALT-H (holding down the
Alt key and press H). The contents of the help text depends on the function which
TB100PP is currently executing.
You can also ask for help about each function, by moving the cursor (the inverted
bar) to the desired function and pressing ALT-H.
The help text will contain the following information :
                           FUNCTION DESCRIPTION       A short description of the functic
                           FUNCTION INPUT             The input which is needed for the
                           FUNCTION OUTPUT            The possible output of the functic
                           PRELIMINARY FUNCTIONS      Some functions need preliminary fu
                           function needs one or more preliminary functions it will be s
                           NOTE                       Miscellaneous help information.
^L
HELP ON READ FUNCTIONS
The READ functions of TB100 are :
                       1.  Read Data,                 to read data from Working Zones.
                       2.  List Directory,            to list the contents of a Data Fil
                       3.  Certify,                   on the one hand can be used for pr
is recorded inside the card memory; on the            other hand, to read (confidential)
in an encrypted            way.
^L
```

NOTES

This fragment of a help file is truncated on the right-hand side, and the page-feed symbols are replaced by "^L", a sequence frequently used by text editors to represent a page-feed.

The Log File

FIGURE A-02 A LOG FILE



```
************************************************************
TB100PP LOGFILE : CREATED 04/11/90, 21:46
************************************************************
21:46                   Function: Open line. Reader name = CR1
                        Result  : Connex = 0, status : 00.
21:46                   Function: Swallow.
                        Result  : p_stat : 60 80
21:46                   Function: Power card.
                        Result  : p_stat : 21 20 00 07 68 90 00
                        Result  : p_stat : 90 00
                        Result  : p_stat : 90 00
                        Result  : p_stat : 90 00
                        Result  : p_stat : 90 00
                        Result  : p_stat : 90 00
                        Result  : p_stat : 90 00
                        Result  : p_stat : 90 00
                        Result  : p_stat : 90 00
                        Result  : p_stat : 90 00
                        Result  : p_stat : 90 00
                        Result  : p_stat : 90 00
21:47                   Function: ANALYSE DATAFILE
+------------------------------------------------------------------------------+
|Type of header          | Ref. ID or          | Start| Stop | Length of       |
| or zone/area           | Key vers.           | Addr.| Addr.| zone in words|
+------------------------------------------------------------------------------+
|Public zone             |  FF                 | 000  | 005 | 006 (6)         |
|ATZ zone                |  6C                 | 006  | 008 | 003 (3)         |
|IK zone                 |   0                 | 009  | 00B | 003 (3)         |
|PIN zone                |   F                 | 00C  | 010 | 005 (5)         |
|SK zone                 |   F                 | 011  | 013 | 003 (3)         |
|Virgin space            | N/A                 | 014   | 29F | 28C (652)       |
|End of Datafile         | N/A                 | 2A0  | 2A0 | 001 (1)         |
+------------------------------------------------------------------------------+
************************************************************
LOGFILE CLOSED 04/11/90, 21:52
************************************************************
```

The log file illustrated above is that resulting from the fllowing sequence of operations:

- Open Log File
- Open Line To Reader
- Swallow Card
- Power Card
- Analyse Data File
- Close Log File

The analysis operation produced the screen output used in Figure 4-14 to illustrate the *Analyse DF* function from the *Power Tools* menu.

5122 995 52631