

CryptoPCcard



PKI Security Modem

CryptoPCcard

PKI Security Modem

11 May 2001
Revision 1.0
US3010 Rev B

NOTICE

Western DataCom reserves the right to make improvements or modifications to the product described in this manual at any time and without notice. While every effort has been made to ensure against any inaccuracies or oversights in this publication, Western DataCom will not be held responsible for loss of information or any direct, indirect or consequential damages arising from the use of the product.

TRADEMARKS ACKNOWLEDGEMENTS

AT is a registered trademark of Hayes Microcomputer Products Inc.
Enhanced Cellular and EC are registered trademarks of Conexant, Inc.
CryptoPCcard is a registered trademark of Western DataCom Co., Inc.
Hayes is a registered trademark of Hayes Microcomputer Products.
Microcom Networking Protocol are trademarks of Microcom Inc.
MNP is a registered trademark of Microcom Inc. Microcom and
MNP is a registered trademark of Microcom Inc.
MS-DOS, Windows and Microsoft are registered trademarks of Microsoft Corporation

Copyright @ 2001 by Western DataCom Co., Inc., All Rights Reserved.

Printed in U.S.A.

<http://www.western-data.com>

TABLE OF CONTENTS

1. Getting Started	1-1
2. Led Indicators	2-1
3. AT Commands	3-1
- Basic AT Commands	3-3
- &Commands	3-9
- % Commands	3-12
- \ Commands	3-13
- Facsimile AT Commands	3-14
- Class 1 Fax Commands	3-15
4. S-Registers	4-1
- S-Register Descriptions	4-2
5. Data Encryption & Security	5-1
Appendix A Troubleshooting and Useful Hints	A-1
Appendix B RS-232 Pinout	B-1
Appendix C ASCII Table	C-1
Appendix D HEX Table	D-1
Appendix E BINARY Table	E-1
Appendix F Specifications	F-1
Appendix G Technical Support	G-1
Appendix H Additional Commands	H-1
Appendix I International Operation	I-1
Appendix J Registration Numbers	J-1

1. GETTING STARTED

The CryptoPCcard Modem is a PCMCIA Type II communications device designed for data transmission and reception. It is compatible with many international protocols and will accept data from your computer equipment at speeds up to 115,200 bps. The CryptoPCcard fits into a standard Type II PCMCIA card slot for desktop or laptop applications.

The CryptoPCcard has been designed to transmit and receive data over standard telephone communications lines in accordance with the following standards/recommendations: CCITT V.90, KFLEX, V.34, V.32 bis, V.32, V.23, V.22 bis, V.22, V.21, Bell 212A and Bell 103. In addition, the CryptoPCcard supports MNP Level 2-4 and V.42 error correction in addition to MNP Class 5 and V.42bis data compression.

In addition to the above features, CryptoPCcard provides for automatic dialing and call progress monitoring, auto-answer capabilities, storage of modem configurations and telephone numbers in non-volatile internal memory, industry-standard AT command set and remote/internal test modes.

CryptoPCcard can also be placed in a mode where it will negotiate the highest possible speed and data compression capability with the remote modem giving you maximum performance and security every time you connect.

The CryptoPCcard Package

CryptoPCcard is shipped with the following items:

- One CryptoPCcard PCMCIA Type II modem
- One International DAA "dongle"
- One RJ-11C telephone cable
- One CryptoPCcard User Manual
- One CryptoPCcard installation diskette

System Requirements

- Any computer system with one unused PCMCIA slot
- Communications software (Dial-up Networking)
- A VGA graphics monitor
- 640K of memory for all modem functions (1 Meg strongly recommended)
- A hard disk for storing files

Connecting your unit

1. Installation varies per operating system. For non Plug-n-Play OS turn power off prior to installing CryptoPCcard in open PCMCIA slot.
2. Connect DAA (dongle) to connector on rear of CryptoPCcard.
3. Load appropriate drivers for CryptoPCcard for particular OS.
4. Connect one end of a RJ11 telephone cable to the CryptoPCcard DAA telephone jack and then the other end to the phone jack on your wall.

You are now ready to install the drivers necessary to operate your the CryptoPCcard modem:

Windows 2000/ME/XP

Windows 2000/ME/XP will automatically detect the insertion of the CryptoPCcard modem. It will load the Microsoft "Standard PCMCIA Driver". Through control panel update driver with Western DataCom supplied inf file (mdmwdc.inf). Accept update with an unsigned driver, driver currently in progress of being signed by Microsoft.

Windows NT

Under control panel select add new hardware, have disk. Insert CryptoPCcard installation diskette and click OK. Select the appropriate model when prompted by Windows. Select default parameters and click finish. Winnt will update remote access service and prompt for a re-boot. This completes the installation under Windows NT.

Windows 98

Windows 98 will automatically detect the insertion of the CryptoPCcard modem. It will load the Microsoft "Standard PCMCIA Driver". Through control panel update driver with Western DataCom supplied inf file (mdmwdc.inf).

Windows 95

Windows 95 will automatically detect the insertion of the CryptoPCcard modem. It will load the Microsoft "Standard PCMCIA Driver". Through control panel update driver with Western DataCom supplied inf file (mdmwdc.inf).

MS-DOS

No drivers are required for operation under MS-DOS.

The A / Command

□ If the characters A/ (instead of AT) are received, CryptoPCcard will re-execute the most recently received command line. In this case, the parity is assumed to be the same as that of the most recently received AT prefix.

Escaping to Command Mode

□ In order to enter an AT command while on-line, the modem must temporarily be placed in command mode. This is done via the escape sequence. CryptoPCcard implements the TIES (Time Independent Escape Sequence). To escape to command mode and enter an AT command, simply type +++ the modem will respond with OK, you can now enter valid AT commands. Returning to on-line mode is done via the ATO command.

Command Line Characters

- All characters that follow the AT prefix are taken to be commands (these are described below).
- The parity bit of all command characters is ignored.
- Spaces (20 Hex) between command characters (and option characters) are ignored.
- No more than 40 command line characters are allowed. If more than this is received, the command line will be ignored and the "ERROR" result code will be returned when the carriage return character is received

The Carriage Return Character

- The carriage return character is used to signify the end of the command line. When this character is received, CryptoPCcard will begin to process the command characters previously received.
- The default value for this character is Control-M (D Hex) but it may be changed through modification of the appropriate S-register.

The Backspace Character

- The backspace character is used to edit the command line. If it is received, CryptoPCcard will ignore the most recently received command character and issue a backspace-space-backspace sequence to the DTE.
- If an attempt is made to backspace onto the AT sequence, CryptoPCcard will ignore the backspace character and take no action.

2. LED INDICATORS

There is 1 LED indicators on the CryptoPCcard DAA front panel. This LED Indicates the operating mode and the connection state:

- DAA:
(RED) The red LED on the DAA "dongle" indicates two states (1) that the CryptoPCcard is in modem mode and (2) that a secure connection is not established or idle.

- DAA:
(GREEN) When the LED is green on the DAA "dongle" it indicates that the CryptoPCcard is (1) in FORTEZZA Crypto PCcard mode or (2) that a secure connection has taken place while in modem mode. See switch position below.

- SWITCH:
(YELLOW) When the micro-switch on the back of the CryptoPCcard is in the Yellow position the CryptoPCcard is operating in Secure Modem Mode. The DAA LED will be lit red when idle and green when secure.

- SWITCH:
(BLUE) When the micro-switch on the back of the CryptoPCcard is in the Blue position the CryptoPCcard is operating in FORTEZZA Crypto Card mode. The DAA LED will be lit green at all times.

The CryptoPCcard has a built in power-on self test routine that is run after being powered on.

Should any error occur the LED will indicate the failure with various patterns. If the user encounters an unidentified pattern please make note of it and recycle power. If the problem continues please contact Technical Support at 440-835-1510.

3. AT COMMANDS

This section discusses the operation of the AT command interpreter as well as describing all AT commands supported by CryptoPCcard.

The AT Command Interpreter

CryptoPCcard implements the industry-standard AT command set. These commands are only available to the user when CryptoPCcard is in command or on-line command mode and are realized in the form of asynchronous characters received from the DTE.

Most users will never find the need to directly use AT commands as these are often handled by the communications software.

The ATprefix

- All command lines must begin with the two letters 'A' and 'T'. Either upper case or lower case is acceptable but both letters should have the same case.
- CryptoPCcard attempts to determine the speed of the 'A' by measuring the duration of its start bit. The 'A' must be received at one of the speeds supported by CryptoPCcard (i.e. 300, 1200, 2400, 4800, 9600, 19200, 38400, 57600 or 115,200 bits/s).
- Once the 'A' and 'T' characters have been received, CryptoPCcard determines the parity of the DTE by analyzing the parity bits of these two characters. All result codes and information text issued by CryptoPCcard will be generated with this parity.

The following asynchronous character formats are supported:

Start Bit	Data Bits	Parity Bit	Stop Bits
1	7	Even or Odd	1
1	7	None	2
1	7	Mark or Space	1
1	8	None	1

- If the CryptoPCcard receives a character but fails to detect it as an 'A', it begins to search for another 'A' character. If CryptoPCcard receives an 'A' but it is not followed by a 'T', CryptoPCcard begins searching for an 'A' again.

L: Speaker Volume

Sets the speaker volume when speaker is on.

L0 - Speaker off.

L1 - Low volume.

L2 - Medium volume

L3 - High volume.

M: Speaker Control

Controls how the speaker behaves when off hook.

M0 - Speaker always off.

M1 - Speaker on until handshake is complete.

M2 - Speaker always on.

M3 - Similar to M1 except speaker is disabled when dialing.

N: Handshaking

Selects whether a connection will be forced to a specific speed.

N0 - Sets the required connection speed to that set under S37.

N1 - allows handshaking at the highest speed supported.

O: Return to On-Line State

Applicable when a physical connection with a remote modem exists and CryptoPCcard is in the on-line command state.

O0 - Returns CryptoPCcard to the on-line state.

O1 - As O0 except that when a 2400 bits/s or higher connection is established an equalizer retrain sequence is transmitted.

P: Pulse Dialing

Causes subsequent dial digits to be executed as pulses.

□ The default value for this character is Control-H (8 Hex) but it may be changed through modification of the appropriate S-register.

Characters Ignored by CryptoPCcard

□ Other than the above characters, all ASCII control characters (value less than 20 Hex) are ignored.

Processing Command Characters

□ CryptoPCcard processes each command character in the sequence that it was received. Any change in operational state required by a command occurs as soon as the command is processed.

□ If an error occurs in the processing of a command, CryptoPCcard will stop processing the command line and output the "ERROR" result code.

□ The detection of an unimplemented command during processing causes a command processing error.

□ Some commands (e.g. E, I, Q, V) may be followed by numeric arguments which select a particular option for that command. If the argument is missing, a value of zero is assumed. If the value is outside the valid range of arguments for that command, a command processing error occurs.

□ If command line processing completes without error, the "OK" result code will be output.

AT Commands Supported by CryptoPCcard

This section discusses the AT commands generally used to handle the transmission of asynchronous data. They are listed in alphabetical order.

<i>BASIC AT COMMANDS</i>

A: Answer mode

Causes CryptoPCcard to go off hook and attempt a handshake in answer mode.

B: Bell/CCITT Mode

B0 - CCITT modulation schemes are used (at 1200 bits/s).

B1 - Bell modulation schemes are used at 1200 bits/s).

D: Dial Number

Instructs CryptoPCcard to go off-hook and execute the dial string which follows the D. Commands which may be part of the dial string are listed below. Any unrecognized character in the dial string is ignored. Once dialing is complete, CryptoPCcard attempts a handshake in originate mode (unless the R parameter is given).

0-9 (any numeric digit) - Causes the indicated digit to be dialed.

A, B, C, D, # or * (tone dial only) - Causes the indicated symbol to be dialed.

P -Causes subsequent numbers to be pulse dialed.

T -Causes subsequent numbers to be tone dialed.

R -Forces CryptoPCcard to dial a call in answer mode.

W -Causes CryptoPCcard to wait for a dial tone using S7 as a time out.

' -Causes a delay, determined by S8, before CryptoPCcard proceeds with the next command or digit.

! -Causes CryptoPCcard to go on-hook for .5 sec and then off-hook for .5 seconds before continuing.

@ -Causes CryptoPCcard to wait until it detects 5 seconds of silence before continuing.

; -Causes CryptoPCcard to go to the command mode when the number is dialed. In order to proceed with channel establishment mode ATO or ATD must be entered. Any characters that follow this parameter are treated as AT commands.

L -Causes the last telephone number that was dialed by CryptoPCcard to be re-dialed.

Sn -Causes CryptoPCcard to dial the number in stored position "n" [format is or Sn].

E: Echo Commands

Defines whether characters are echoed back from CryptoPCcard to the DTE when in command mode.

E0 -Command echo disabled.

E1 -Command echo enabled.

F: Set DCE Speed

F0 - Match DTE

F1 - 2400bps

F2 - 4800bps

F3 - 7200bps

F4 - 9600bps

F5 - 12000bps

F6 - 14400 bps

F7 - 16800 bps

F8 - 19200 bps

F9 - 21600 bps

F10- 24000 bps

F11- 26400 bps

F12- 28800 bps

F13 - 31200 bps

F14 - 33600 bps

H: Hook Switch Control

Controls the hook switch relay of CryptoPCcard.

H0 - Causes CryptoPCcard to go on-hook.

H1 - Causes CryptoPCcard to go off-hook.

In error correction mode S38 dictates the delay before going on-hook.

I: Interrogate CryptoPCcard Status

I0 - Requests CryptoPCcard product code.

I1 - Requests the checksum of the EEPROM.

I2 - Returns Product Serial Number.

I3 - Returns CryptoPCcard Firmware Revision.

I4 - Reports Product Identifier Label

I5 - Reports Country Code Parameter.

I6 - Reports modem data pump model, internal code.

I7 - Report DAA code.

& K: Flow Control

Defines the flow control options

- &K0** - Local flow control is off.
- &K3** - **Hardware Flow Control [RTS/CTS].**
- &K4** - Software Flow Control [Local XON/XOFF]. In this mode CryptoPCcard recognizes and transmits the XON/XOFF characters from and to the DTE in order to start or stop data. CryptoPCcard will not transmit the XON/XOFF characters received from the DTE to the remote modem.
- &K5** - Software Flow Control [Local/Transparent XON/XOFF]. In this mode CryptoPCcard recognizes and transmits the XON/XOFF characters from and to the DTE in order to start or stop data. CryptoPCcard will also transmit the XON/XOFF characters received from the DTE to the remote modem.

&S: Data Set Ready Options

Defines how the DSR signal is handled by the MDMC.

- &S0** - **DSR is always ON**
- &S1** - DSR is compatible with CCITT recommendations. In command mode DSR is OFF. When originating a call DSR forced ON when CryptoPCcard receives a 2100 Hz (or 2225 Hz) answer tone, or (if this is absent) when valid carrier is detected. When answering a call DSR is forced ON during handshaking as defined by V.25.

&T: Test Commands

- &T0** - Test currently in progress is terminated.
- &T1** - Local analog loopback test is initiated (CCITT V.54).
- &T3** - Local digital loopback test is initiated.
- &T4** - Allows CryptoPCcard to respond to a request (from remote modem) for a Remote Digital Loopback.
- &T5** - Prohibits CryptoPCcard from granting a request (from the remote modem) for a Remote Digital Loopback.
- &T6** - Remote digital loopback test (CCITT V.54) when on-line.

Q: Return Result Codes

Defines whether or not CryptoPCcard will issue result codes to the DTE.

- Q0** - **Result codes returned.**
- Q1 - Result codes not returned.

T: Tone dialing

Causes subsequent dial digits to be executed as DTMF tones.

V: Verbose mode

Defines the form of result codes returned by CryptoPCcard.

- V0 - Terse form responses enabled. (Numeric responses)
- V1** - **Verbose responses enabled (English responses).**

W: Connection Result Codes

Defines how connect messages are returned by the CryptoPCcard.

- W0** - **Upon connect reports DTE speed.**
- W1 - Upon connect reports line speed, error correction protocol and DTE speed.
- W2 - Upon connection reports DCE speed.

X: Extended Response Codes

Defines the GSTN network tones which are recognized by CryptoPCcard.

- X0 - Causes CryptoPCcard to ignore any network tones and omit the connection speed message.
- X1 - As above but enables the connection speed result codes.
- X2 - Causes CryptoPCcard to detect dial tone.
- X3 - Causes CryptoPCcard to detect busy tone.
- X4** - **Causes CryptoPCcard to detect busy and dial tones.**

Y: Long Space Disconnect

Y0 - Disabled.

Y1 - Enabled.

When set for Y1, on-line and not in error correction: CryptoPCcard will disconnect if it receives a continuous "break" from the remote modem for a period of time greater than or equal to 1.6 seconds. As well, when CryptoPCcard is instructed by the DTE to hang up it will send a 4 second break to the remote modem prior to going on hook.

Z: Software Reset

The user configuration stored in non-volatile memory is recalled to become the active configuration.

Z0 - Resets CryptoPCcard and recalls user profile 0.

Z1 - Resets CryptoPCcard and recalls user profile 1.

& COMMANDS

& C: Data Carrier Detect Options

Defines what CryptoPCcard outputs as the DCD signal on the DTE interface.

&C0 - The interface control signal DCD is always ON.

&C1 - **DCD (Carrier) follows true state of carrier.**

& D: Data Terminal Ready Options

Defines how the DTR signal is interpreted by CryptoPCcard. If S25 is not zero the DTR signal is ignored for S25 seconds after a call is indicated (See S25 definition).

For asynchronous mode:

&D0 - DTR is ignored.

&D1 - DTR drop is interpreted according to the current &Qn setting as follows:
&Q0,1,4,5,6, DTR drop is seen as an escape sequence had been entered.

&Q2,3 DTR drop causes modem to hang-up. Auto answer is inhibited.
&D2 - **DTR drop is interpreted according to the current &Qn setting as follows: &Q0 thru &Q6 DTR drop causes modem to hang up.**

&D3 - DTR interpreted according to &Qm setting as follows:
&Q0,1,4,5,6 DTR drop causes the modem to perform a soft reset as if the Z command were received.
&Q2,3 DTR drop causes modem to hang-up. Auto answer is inhibited.

& F: Set Factory Defaults

Sets S-registers to factory default values indicated in **BOLD**.

FACSIMILE AT COMMANDS SUPPORTED BY CRYPTOCOM

The CryptoPCCard does have the ability to operate in facsimile mode. Due to its non-secure operating mode Fax support for the CryptoPCCard has been disabled. Please disregard this section of the User Manual.

General Comments on Fax AT Commands

□ All commands require the AT prefix and are generally entered in the same way as the data modem AT commands.

□ All commands except "+FTS" and "+FRS" support a syntax of the form "+ < COMMAND > X" where X may be any of three different strings. The string "=" is used to provide a value for execution by the command. The string "=?" is used to interrogate the command as to its range of acceptable values (i.e. the command returns a string of comma-separated values that are those that can be provided to the command via the "=" string). The string "?" is used to determine the value for that command that is currently in use.

□ All commands except "+FCLASS" cause a command processing error if received when CryptoPCCard is on hook.

□ The transmit and receive facsimile commands require a modulation parameter <MOD>. Below is a list of the possible values of <MOD>.

Short training Sequence

<MOD>	Modulation Type	Speed (bits/s)
3	V.21 ch.2	300
24	V.27 ter	2400
48	V.27 ter	4800
72	V.29	7200
73	V.17	7200
74	V.17 w/st	7200
96	V.29	9600
97	V.17	9600
98	V.17 w/st	9600
121	V.17	12000
122	V.17 w/st	12000
145	V.17	14400
146	V.17 w/st	14400

&T7 - Remote digital loopback test with self-test is initiated (CCITT V.54) when on-line.

&T8 - Local analog loopback with self-test is initiated (CCITT V.54).

&V: Display Stored Parameters

Causes CryptoPCCard to display the current and pre-stored configuration profiles.

&V0 - Display current configuration and store profiles

&V1 - Displays last connection status

&W: Save Registers Command

Saves the current register settings

&W0 - Stores configuration in profile 0

&W1 - Stores configuration in profile 1

&Z: Store Number Command

Store the desired telephone number in location 0 through 3. The maximum length of each stored number is 32 digits. The format of the stored number is identical to that accepted by the D command.

&Zn=x Where x is the telephone number to be stored in position n.

% COMMANDS

% C: Data Compression

- %C0** - Compression off (same as &U0).
- %C1** - **Compression On (same as &U1).**

%E: Auto Retrain

Auto retrain determines whether CryptoPCcard will suspend transmission and send a retraining sequence if line conditions deteriorate. Connect speed optimization determines whether CryptoPCcard will adjust the line speed(down only in the absence of a retrain) if the line conditions deteriorate.

- %E0** - Disable auto retrain and connect speed optimization.
- %E1** - Enable auto retrain.
- %E2** - **Enable connect speed optimization.**
- %E3** - Enable both auto retrain and connect speed optimization.

% L: Receive Level in dB

Returns a value(9-43) which represents the Receive Level in dB(e.g., a value of 10 indicates that the receive level is -10dB).

% Q: Return Line Signal Quality

Returns the value(0-127) of the most significant byte of the eye quality monitor

\ COMMANDS

\ G: Modem-to-Modem Flow Control During a Normal Connection

- \G0** - **No modem-to-modem flow control.**
- \G1** - Use modem-to-modem software flow control (XON / XOFF).

\ K: Break Handling

- \K0** - Enter on-line command mode, no break sent to remote modem
- \K1** - Clear data buffers and send break to remote modem.
- \K2** - Same as 0.
- \K3** - Send break to remote modem immediately.
- \K4** - Same as 0
- \K5** - **Send break to remote modem in sequence with transmitted data.**

\ N: Operational Mode

- \N0** - Selects normal speed buffer modem (disables error-correction).
- \N1** - Selects direct mode.
- \N2** - **Selects reliable (error correction) mode.**
- \N3** - Selects Auto-reliable mode (fallback to non error correction).
- \N4** - Selects LAPM error-correction mode (V.42bis).
- \N5** - Selects MNP5 error-correction modem.

S-REGISTER DESCRIPTIONS

The complete set of S-registers is listed below with the corresponding bit maps where applicable. All values are in decimal format. Default values indicated in bold type are those written after execution of the &F command (factory default). If the register TYPE is non-storable then this default value will also be written whenever CryptoPCcard is reset. For storable registers, however, the value after reset will be set to that stored in the appropriate stored profile.

Any register not specifically mentioned below is reserved.

S0: Rings To Answer On

0 = No auto answer
Any other = CryptoPCcard answers after this number of rings
Default = 0
TYPE: Storable

S1: Ring Count

This register is reset to 0 if 8 seconds elapse since receipt of the previous ring
Default = 0
TYPE: Non-Storable, read only

S2: Escape Sequence Character

If the value is greater than 127, escape sequence is disabled
Default = 43 (+)
TYPE: Storable

S3: Carriage Return Character

Value: 0 - 127
Default = 13 (ASCII CR)
TYPE: Storable

S4: Line Feed Character

Value: 0 - 127
Default = 10 (ASCII LF)
Type: Storable

CLASS 1 FAX COMMANDS

+FCLASS: Identify Service Class

This command selects whether CRYPTOCOM is configured as a data or fax modem.

+FCLASS=0 - CryptoPCcard configured as data modem.
+FCLASS=1 - CryptoPCcard configured as Class 1 fax modem.
+FCLASS=2 - CryptoPCcard configured as Class 2 fax modem.

+FTS: Stop Transmission and Wait

Transmission is halted followed by a wait for the specified time.

+FTS=<TIME> - Wait for the time (in increments of 10 ms) specified by <TIME> 0 - 2.55 s).

+FRS: Receive Silence

This command completes execution when silence is detected from the remote modem for the specified amount of time. Processing of the command is aborted, without error, if a character is received from the DTE while attempting to detect the period of silence.

+FRS=<TIME> - Wait for the time (in increments of 10 ms) specified by <TIME> (0 - 2.55 s).

+FTM: Transmit Facsimile Data

A physical connection with the modulation type specified by <MOD> is first established, Data received from the DTE is then transmitted in facsimile format.

+FTM=n - Transmit facsimile data using modulation <MOD>.

see table on page 3-16

+FRM: Receive Facsimile Data

A physical connection with the modulation type specified by <MOD> is attempted with the remote modem. If this succeeds, data subsequently received from the remote modem is sent to the DTE in facsimile format. If the physical connection fails, the "+FCERROR" result code is returned.

+FRM=n - Receive facsimile data using modulation <MOD>.

see table on page 3-16

+FTH: Transmit Facsimile Data HDLC

A physical connection with the modulation type specified by <MOD> is first established. Data received from the DTE is then transmitted in facsimile format using HDLC framing.

+FTH=n - Transmit facsimile data, HDLC format, using modulation <MOD>.

see table on page 3-16

+FRH: Receive Facsimile Data HDLC

A physical connection with the modulation type specified by <MOD> is attempted with the remote modem. If this succeeds, data subsequently received from the remote modem, using HDLC framing, is sent to the DTE in facsimile format. If the physical connection fails, the "+FCERROR" result code is returned.

+FRH=n - Receive facsimile data, HDLC format, using modulation <MOD>.

MODULATION TABLE	
n Value	Modulation Scheme
3	V.21 channel 2 300 bps
24	V.27 ter 2400 bps
48	V.27 ter 4800 bps
72	V.29 7200 bps
73	V.17 7200 bps long
74	V.17 7200 bps short
96	V.29 9600 bps
97	V.17 9600 bps long
98	V.17 9600 bps short
121	V.17 12000 bps long
122	V.17 12000 bps short
145	V.17 14400 bps long
146	V.17 14499 bps short

4. S-REGISTERS

S-registers are byte-wide locations in CryptoPCcard memory that contain information about the configuration and operational status of CryptoPCcard. Some of the more relevant S-Registers are shown on the following pages. Many of CryptoPCcard's options can be directly set via the S-registers and some extended features are only available through setting of these registers.

Some S-registers are bit-mapped, that is, the individual bits (or, sometimes, groups of bits) contain significant information as opposed to the contents of the register as a whole. When references to bit-mapped registers are made, the least significant bit is bit 0 while the most significant bit is bit 7.

Reading an S-register

□ To display the value of an S-register in decimal format the command Sn? is used where 'n' references the desired register.

Writing an S-register

□ An S-register's value may be altered by the Sn=X command where 'n' is the register to be changed and 'X' is the new decimal value to be assigned to it.

Defaults

□ Entering AT? will display the content on the last register accessed while AT=n will alter the last accessed S register with the decimal value 'n'

□ If the Sn=X command is used and the value 'X' is not given, zero will be written to the appropriate S-register.

□ Unless otherwise specified, any value between 0 and 255 (decimal) may be written to an S-register. Out of range values are rejected and cause a command processing error.

- Bit 5 RLSD (DCD) behavior (&Cn)
 0 = DCD always on, &C0 selected
 32 = DCD normal. &C1 selected
- Bit 6 DSR control (&Sn)
 0 = DSR always on, &S0 selected
 64 = &S1 selected
- Bit 7 Long space disconnect (&Yn)
 0 = Disabled
 128 = Enabled
- TYPE: Storable

S22: Bit-mapped

- Bit 1,0 Speaker volume control (Ln)
 0 = off (L0)
 1 = Low (L1)
 2 = Medium (L2)
 3 = High (L3)
- Bit 3,2 Speaker control (Mn)
 0 = Always off (M0)
 4 = On until carrier detected (M1)
 8 = Always on when off hook (M2)
 12 = Off during dialing and after carrier detected (M3)
- Bit 6,5,4 Extended response codes (Xn)
 0 = Ignore GSTN status and do not report connection
 speed - (X0)
 64 = As for X0 and also report connection speed -
 (X1)
 80 = Detect dial tone and report connection speed -
 (X2)
 96 = Detect busy tone and report connection speed
 (X3)
 **112 = Detect dial and busy tones and report
 connection speed - (X4)**
- Bit 7 Reserved
- TYPE: Storable

S5: Backspace Character

Value: 0 - 255
Default = 8 (ASCII BS)
 TYPE: Storable

S6: Wait Time Before Dialing

Value: 2 - 255 s
Default = 2
 TYPE: Storable

S7: Wait Time For Carrier/Dial Tone

Value: 1 - 255 s
Default = 50
 TYPE: Storable

S8: Duration for Pause (,) Dial Modifier

Value: 0 - 255 s
Default = 2
 TYPE: Storable

S9: Carrier Detect Response Time

Value: 1 - 255 in 0.1 s increments (.1 - 25.5 s)
Default = 6
 TYPE: Storable

S10: Delay Between Lost Carrier And Hang Up

Value: 1 - 255 in 0.1 s increments (.1 - 25.5 s)
Default = 14
 TYPE: Storable

S11: DTMF Tone Duration

Value: 50 - 255 in 0.001 s increments (.05 - .255 s)
Default = 95
 TYPE: Storable

S12: Escape Prompt Delay

Value: 0 - 255 in 0.02 s increments (0 - 5.1 s)

0 = Do not check Escape Prompt Delay

Default = 50

TYPE: Storable

S14: Bit-mapped

- Bit 0 This bit is ignored
- Bit 1 Echo command characters (En)
0 = Disabled (E0)
2 = Enabled (E1)
- Bit 2 Generate result codes (Qn)
0 = Send result codes (Q0)
4 = Do not send result codes
- Bit 3 Verbose/numeric result codes (Vn)
0 = Numeric (V0)
8 = Verbose (V1)
- Bit 5 Tone (T)/ Pulse (P)
0 = Tone dialing (T)
32 = Pulse dialing (P)
- Bit 6 Reserved
- Bit 7 0 = Answer mode
128 = Originate mode
- TYPE: Storable

S16: Test Status (Bit-mapped)

Indicates the test in progress status:

- Bit 0 Local Analog Loopback (&T1)
0 = No ALB
1 = ALB active (&T1)
- Bit 1 Reserved

- Bit 2 Local Digital loopback (&T3)
0 = No DLB
4 = DLB active (&T3)
- Bit 3 Status of Remote Digital Loopback
0 = Modem not in RDL
8 = RDL in progress
- Bit 4 Remote digital loopback requested (&T6)
0 = RDL not requested
16 = RDL requested (&T6)
- Bit 5 RDL with self test (&T7)
0 = Disabled
32 = Enabled
- Bit 6 Local Analog Loopback with self test (&T8)
0 = Disabled
64 = Enabled
- Bit 7 Not Used
- TYPE: Non-Storable

S18: Test Timer

Value: 0 - 255 s

0 - Infinite test time

Any other = Test is terminated after specified time elapses

Default = 0

TYPE: Storable

S21: Bit-mapped

- Bit 0 Reserved
- Bit 1 Reserved
- Bit 2 CTS Behavior (&Rn)
0 = CTS tracks RTS (&R0)
4 = CTS always on (&R1)
- Bit 3,4 DTR control (&Dn)
0 = Ignore (&D0)
8 = Command state (&D1)
16 = Hang up (&D2)
24 = Reset (&D3)

S23: Bit-mapped

Bit 0 Grant RDL
0 = RDL not allowed (&T5)
1 = RDL allowed (&T4)

Bit 3,2,1 DTE Rate
0 = 300
1 = 600
2 = 1200
3 = 2400
4 = 4800
5 = 9600
6 = 19200
7 = 38400 or higher

Bit 5,4 Parity
0 = Even
16 = not used
32 = Odd
48 = None

Bit 7,6 Reserved

TYPE: Storable

S24: Sleep Inactivity Timer

Value: 0 - 255 in 1 s increments (0 - 255 s)

Default = 0

TYPE: Storable

S25: DTR Detection

Value: 0 - 255 in 0.01 s increments (0 - 2.55 s)

Default = 5

TYPE: Storable

S27: Bitmapped

Bit 6 Bell / CCITT (B CMD)
0 = CCITT
64 = Bell

TYPE: Storable

S30: Disconnect Inactivity Timer

Value: 0 - 255 in 10 s increments (10 - 2550 s)
0 - timer disabled

Default = 0

Type: Storable

S39: Bit-mapped

Bits 2,1,0 DTE flow control

0 = No DTE flow control

3 = RTS/CTS (&K3)

4 = XON/XOFF (&K4)

5 = XON/XOFF transparent (&K5)

TYPE: Storable

S41: Bitmapped

Bits 0-1 Compression selection (%Cn)

0 = Disabled (%C0)

1 = MNP 5 (%C1)

2 = V.42 bis (%C2)

3 = MNP 5 and V.42 bis (%C3)

Bits 2,6 Auto retrain and fallback/fall forward (%En)

0 = Disable (%E0)

4 = Retrain enabled (%E1)

8 = Fallback/Fall Forward enabled (%E2)

TYPE: read only

5. Data Encryption & Security

The Western DataCom (WDC) CryptoPCcard is a NIST Skipjack/3DES/AES encryption modem designed and manufactured to be compliant with Security Level 2 of Federal Information Processing Standards Publication(FIPS PUB 140-1): **Security Requirements for Cryptographic Modules.**

To operate the CryptoPCcard certain security parameters must be loaded to negotiate a secure connection over public switched telephone networks. All security parameters are programmed using a Certificate Authority Workstation. They can be programmed by Western DataCom for commercial usage or by the National Security Agency for defense applications with a required clearance of up to "SECRET". Once the cards are programmed there are several commands used to configure the modem for operation.

!C PIN Command

The **!C** command is used to set the User PIN of a particular modem. This User PIN is used to enable the modem for a secure connection attempt, its format is:

AT!C=xxxxxx

where x is the 4 to 12-character Numeric User PIN.

!L List KMID Command

The **!L** command is used to display the KMID list stored in the modem, its format is:

AT!L

the output will be a listing of up to 64 slots loaded with specific key information for secure connections.

!S Command

The !S command is used to set the Personality (KMID). The KMID is used to establish secure connections, its format is:

AT!Sxxxxxxxxxxxxxxxx

Please note: the !S command can be used manually but it is recommended that CertDB be used to configure the modems.

CertDB is a Windows 95 application that simplifies the configuration of the modems.

!Y Command

The !Y command is used to store public key information in the modem and is used in conjunction with the !S command, it's format is:

AT!Y=xxxxxxxxxxxxxxxx

again this command can be used manually but it is recommended that the user use CertDB to configure the modems for secure operation.

For more information regarding CertDB please refer to the application itself and to the user manual contained on the setup disk for the CryptoPCcard.

Technical Support

Western DataCom would like to thank you for purchasing its products. We strive to provide products that will remain reliable through out their lifecycle. All products are warranted for 12-months from the date of purchase to be free of defects. Western DataCom also provides free technical support for the lifetime of the product.

To contact our technical support team please use one of the following methods:

Toll Free: 800-262-3311

International: +01 440-835-1510

Internet: <http://www.western-data.com>

Email: support@western-data.com

Fax: +01 440-835-9146

Troubleshooting and useful hints

In the unlikely event that you experience a problem with your CryptoPCcard modem, please first attempt to identify it in the following list.

If the Modem does not respond to AT commands are:

- Make sure the COM port setting of the modem and communications software does not conflict with another peripheral in your computer.
- Make sure that a supported character format has been selected.
- Make sure that local character echo is on (ATE command)

If the Modem responds with NO DIAL TONE:

- Make sure that the phone line is properly connected between the wall jack and the modem.

If you are unable to get an MNP/V.42 connection:

- The remote modem may not be able to support this mode.
- Make sure the modem has been set for this mode.

If the connection drops immediately after the connection message is displayed:

- Make sure that the PIN's are set on both modems attempting to communicate.

If you see garbage data on the screen after a connection has been established:

- Make sure that the data and parity format selected matches that of the remote modem.
- Make sure that the encryption keys are set the same on both communicating modems.

If you get single bursts of errors on your screen:

- The line condition may be poor. Try using error correction.
- Make sure, if your line has call waiting, that you disable before every modem call.

If you observe problems during a file transfer:

- Make sure that the modem's flow control type setting (AT&K command) is in accordance with that of the communications software.

Hints

- Use the CryptoPCcard default configuration whenever possible..

APPENDIX B

Additional Configuration Commands

The CryptoPCcard has to many AT commands to list in this manual. The commands shown in the previous sections are the most relevant for the everyday user. The following are a few commands that may be of help in configuring the modem:

+MS Command

The +MS command is used to force the modem to connect at a certain speed using a particular protocol (i.e. 9600 - V.32bis). The ability to force various connection speeds with certain protocols can be advantageous for various applications. Its format is:

AT+MS[<carrier>][<automode>][<min_tx_rate>][<max_tx_rate>][<min_rx_rate>][<max_rx_rate>]

Modulation	<carrier>	Possible min_/max_ Rates in Bps
Bell 103	B103	300
Bell 212	B212	1200 Rx/75Tx or 75Rx/1200Tx
V.21	V21	300
V.22	V22	1200
V.22bis	V22B	2400 or 1200
V.23	V23C	1200
V.32	V32	9600 or 4800
V.32bis	V32B	14400, 12000, 9600, 7200 or 4800
V.34	V34	33600, 31200, 28800, 26400, 24000, 21600, 19200, 16800, 14400, 12000, 9600, 7200, 4800 or 2400
V.90	V90	56000, 54667, 53333, 52000, 50667, 49333, 48000, 46667, 45333, 42667, 41333, 40000, 38667, 37333, 36000, 34667, 33333, 32000, 30667, 29333, 28000
K56flex	K56	56000, 54000, 52000, 50000, 48000, 46000, 44000, 42000, 40000, 38000, 36000, 34000, 32000

APPENDIX C

SPECIFICATIONS

- Protocols: V.90, K56flex, V.34bis, V.34, V.32bis, V.32, V.23, V.22bis, V.22, V.21, Bell 212 and Bell 103
- Non-Secure Transmission rate: 56,000 bps, 54,000 bps, 52,000 bps, 50,000 bps, 48,000 bps, 46,000 bps, 44,000 bps, 42,000 bps, 40,000 bps, 38,000 bps, 36,000 bps, 34,000 bps, 33,600bps, 32,000 bps, 31,200bps, 28,800bps, 26,400bps, 24,000bps, 21,600bps, 19,200bps, 16,800bps, 14,400bps, 12,000bps, 9600 bps, 7200bps, 4800bps, 2400bps, 1200bps, 1200bps/75bps, 600bps, 300bps.
- Secure Transmission rate: 33,600 bps, 31,200 bps, 28,800 bps, 26,400 bps, 24,000 bps, 21,600 bps, 19,200 bps, 14400 bps, 12000 bps, 9600 bps, 7200 bps, 4800 bps, 2400 bps, 1200 bps, 300 bps.
- Default transmit level: -9 dBm ± 1 dBm
- Receive signal frequency tolerance ±7Hz
- Receive sensitivity: 0 dBm to -43 dBm
- Rate tolerance ±/-0.01 %
- Flow control: RTS/CTS, XON/XOFF
- Data format: 7 data bits with mark, space or odd parity and 1 or 2 stop bits; 8 data bits with no parity and 1 or 2 stop bits
- Communication medium: 2 wire dial-up or lease line
- Hardware requirements: Computer or terminal with serial RS-232 port
- Typical power consumption: 750 mW

Registration Numbers:

Complies with FCC Part 68

FCC Part 15 Class A - #6FUSA-33272-MD-E
and #6FEUSA-32325-PT-E

UL Listed, TBR21 Registered, CE 0560X