

Diamond 650 Card Reader firmware specifications

Firmware v1.8x



CJS Technology Limited

Date 23rd June 2006

Page 1 of 16

Overview

The v1.8x firmware is intended to allow a high degree of flexibility and control over your contactless smartcard hardware whilst retaining a simple and intuitive command set.

Communications Interface

Host comms is serial running at 115200 baud (factory default), 8 data bits, no parity, 1 stop bit (115200,n,8,1). No flow control has been implemented. USB readers are driven via a virtual com port or by using the relevant DLL for direct access to the device. In all cases, the communications between host and reader remain the same.

Protocols

There are two modes of communication with the reader.

- 1) ASCII
- 2) Binary

These are described below.

ASCII

The reader defaults to this state on power up, reset and after every instruction unless locked out. This mode of operation is suitable for use with a terminal emulator such as HyperTerminal. Ascii commands have the following format:

CMD	P1	P2	<CR>
-----	----	----	------

Where:

CMD is the command character

P1 is the first parameter (where required). There must be a space between CMD and P1

P2 is the second parameter (where required). There must be a space between P1 and P2

Note that P2 may be any number of characters (n) representing n/2 bytes.

<CR> is character 0x0D, and can be generated by pressing the <return> or <enter> key in HyperTerminal.

All parameters are to be supplied in hexadecimal, where 2 characters represent one byte.

In response, you will receive:

RES	LEN	RD	<CR>	<LF>
-----	-----	----	------	------

Where:

RES is the result code. **00** denotes success.

LEN is the length (in bytes) of RD

RD is the Returned Data (if any).

The reader will return an ASCII mode response if presented with an ASCII mode command.

Diamond 650 Card Reader firmware specifications

Firmware v1.8x

Date 23rd June 2006
Page 2 of 16



Binary

Binary commands from the host should have the following format:

STX	LEN	CMD	P1	P2	CSUM	ETX
0x02						0x03

Where:

STX is the 'Start of Text' character 0x02

LEN is the length (in bytes) of CMD + P1 + P2

CMD is the command character

P1 is the first parameter (where required). May be one or two bytes depending on the command, high byte first.

P2 is the second parameter (where required), may be any number of bytes as required.

CSUM is the checksum character generated by XORing all previous bytes starting with <C>.

ETX is the 'End of Text' character 0x03.

In response, the reader will reply in the form:

STX	RES	LEN	RD	CSUM	ETX
0x02					0x03

Where:

STX is the 'Start of Text' character 0x02

RES is the result code. **00** denotes success.

LEN is the length (in bytes) of <RD>

RD is the Returned Data, if any.

CSUM is the checksum character generated by XORing all previous bytes starting with <R>.

ETX is the 'End of Text' character 0x03.

The reader will return a Binary mode response if presented with a Binary mode command. The reader will wait for up to 35ms between characters in a command string before failing with a timeout error.

Binary mode commands are protected against a variety of different failure modes, and should be employed exclusively by the host device in 'real' / mission critical operations. ASCII mode is only provided as a quick and intuitive means of communicating with the reader for development purposes.

Diamond 650 Card Reader firmware specifications

Firmware v1.8x

Date 23rd June 2006
Page 3 of 16



Communicating with the reader

After power up or reset, the reader sends the following text to the serial port:

STX	RES	LEN	CSUM	ETX
0x02	0xFF	0x00	0xFF	0x03

CLS
0x0C

	VER		IDNUM		ST		
Diamond v	n.nn	ID.	nnnn	S	nn	0x0D	0x0A

>

The reader firmware version will be displayed in place of VER.

The reader ID number will be displayed in place of IDNUM

The results of the last selftest will be displayed in place of ST

The user may now enter commands as described in the following pages. All Ascii commands should be terminated with a CRLF.

Reader return codes are as follows:

- 0 - Success
- 1 - Command timeout failure (binary mode only)
- 3 - Command checksum failure or no ETX (binary mode only)
- 4 - Unrecognised command
- 5 - Parameter value error or T = CL start session failure

Other values – Card removed from reader or key Access conditions / keys unacceptable

Diamond 650 Card Reader firmware specifications

Firmware v1.8x



CJS Technology Limited

Date 23rd June 2006

Page 4 of 16

- A x** Defines the key Access conditions for Mifare cards.
x Ascii - up to 2 digit hex value. Binary – a 1 byte integer.

Send Example

ASCII

>A 01 <CR>

Binary

STX	LEN	CMD	P1	CSUM	ETX
0x02	0x02	0x41	0x01	0x40	0x03

Return Example

ASCII

00 00<CR>

Binary

STX	RES	LEN	CSUM	ETX
0x02	0x00	0x00	0x00	0x03

Set the Access conditions for reading and writing to a Mifare 1K or 4K card using this command, as follows:

- 0 = Read and write with key A
- 1 = Read with key B and write with key A
- 2 = Read with key A and write with key B
- 3 = Read and write with key B
- 4 = Derive a suitable strategy (tries Key A then key B) (Default)

The access conditions in the trailer block of each sector of a Mifare (1K & 4K) card define which keys are expected to be used for reading and writing the blocks in that sector. This parameter should match the settings on the card, so if (say) the card expects you to read with key A and write with key B, the Access Condition parameter supplied to the reader should be 02.

This parameter is not stored in non-volatile memory and will be lost when the reader is switched off or reset. It should be defined explicitly if the default (mode 4) is not suitable. Note that reading/writing a card using key Access mode 4 may involve an extra 5ms delay per operation for key derivation compared with the more specific key Access settings.

There does not need to be a card on the reader for this command to be used.

See also commands M (the Mode command), K (the Key command) and D (the Dynamic key command).

Diamond 650 Card Reader firmware specifications

Firmware v1.8x



CJS Technology Limited

Date 23rd June 2006

Page 5 of 16

D x Defines a Keypset for immediate use (for Mifare cards). This keyset is not stored in non-volatile memory and will be lost when the reader is switched off or reset. It is intended for use in systems where the keys are diversified and cannot be pre-loaded into the reader.

X 12 digits 6 digits key A, 6 digits key B.

The dynamic key is only used when mode 2 is selected (see the Mode command for further details)

Send Example

ASCII

>D 0A2122336445C6F70812A1B2 <CR>

Binary

STX	LEN	CMD	P1	CSUM	ETX
0x02	0x0D	0x44	0x0A 0x21 0x22 0x33 0x64 0x45 0xC6 0xF7 0x08 0x12 0xA1 0xB2	0x67	0x03

Return Example

ASCII

00 00<CR>

Binary

STX	RES	LEN	CSUM	ETX
0x02	0x00	0x00	0x00	0x03

There does not need to be a card on the reader for this command to be used.

See also commands M (the Mode command), K (the Key command) and A (the key Access conditions command).

Diamond 650 Card Reader firmware specifications

Firmware v1.8x



Date 23rd June 2006
Page 6 of 16

E x Sets the Energy saving mode.
X Ascii - up to 2 digit hex value. Binary – a 1 byte integer.

Send Example

ASCII
>**E 01** <CR>

Binary

STX	LEN	CMD	P1	CSUM	ETX
0x02	0x02	0x45	0x01	0x44	0x03

Return Example

ASCII
00 00<CR>

Binary

STX	RES	LEN	CSUM	ETX
0x02	0x00	0x00	0x00	0x03

Set the Energy saving mode as follows:

0 = No energy saving
1 = Shut down the RF field when no card present (ie, at the end of an unsuccessful **V** command)
(Other values reserved for future use)

When enabled, this facility reduces the current consumption of the reader and the heat dissipation of the power regulator.

This parameter is not stored in non-volatile memory and will be lost when the reader is switched off or reset. It should be defined explicitly if the default value (1) is not suitable.

There does not need to be a card on the reader for this command to be used.

Diamond 650 Card Reader firmware specifications

Firmware v1.8x

Date 23rd June 2006
Page 7 of 16



I Returns the reader terminal (or ID) number.

Send Example

ASCII
>**I** <**CR**>

Binary

STX	LEN	CMD	CSUM	ETX
0x02	0x01	0x49	0x49	0x03

Return Example

ASCII
00 02 12 34 <**CR**>

Binary

STX	RES	LEN	RD	CSUM	ETX
0x02	0x00	0x02	0x12 0x34	0x24	0x03

There does not need to be a card on the reader for this command to be used.

See also the T command.

Diamond 650 Card Reader firmware specifications

Firmware v1.8x



CJS Technology Limited

Date 23rd June 2006

Page 8 of 16

K x y Defines a Keypset for permanent storage (for Mifare cards). This enables the card reader to read and possibly write Mifare cards using a variety of different keys.

X 2 hex digits / 1 byte 00-27 defines the keyset number (up to 40 keysets)

Y 24 digits / 12 bytes 6 bytes key A, 6 bytes key B.

Up to 40 different keysets can be accommodated by any given reader, these are saved in non-volatile memory in a specific address designated by parameter X. When a card is presented to the reader for read/write, it will use keys as follows:

Mode=0 - Each of the first 8 keysets (0-7) is tried in turn until a match is found and the operation succeeds, or the keysets run out and the operation fails.

Mode=1 – The keyset relevant to the sector involved is tried. Sector 0 uses key 0, sector 3 uses key 3 etc..

Mode=2 – The Dynamic keyset (as loaded by the D command) is used, Keypsets defined with the K command are ignored.

Send Example

ASCII

>**K 0 0A2122336445C6F70812A1B2** <CR>

Binary

STX	LEN	CMD	P1	P2	CSUM	ETX
0x02	0x0E	0x4B	0x00	0x0A 0x21 0x22 0x33 0x64 0x45 0xC6 0xF7 0x08 0x12 0xA1 0xB2	0x6C	0x03

Return Example

ASCII

00 00<CR>

Binary

STX	RES	LEN	CSUM	ETX
0x02	0x00	0x00	0x00	0x03

NB. The keys used may be unique to your organisation and should be treated as highly confidential. Unless you are issuing dynamic keysets, then as a minimum your reader will require one keyset to be entered (as keyset 0 once only). You should not use this command thereafter without being entirely sure you know what you are doing. There does not need to be a card on the reader for this command to be used.

Note that the keysets are stored in non-volatile memory. To avoid premature failure of the non-volatile memory, do not make frequent changes to the keysets. Stored keysets are intended to be fixed. For a keyset which changes frequently, you should use Mode 2 and the Dynamic keyset.

See also commands D (the Dynamic Key command), M (the Mode command) and A (the key Access conditions command).

Diamond 650 Card Reader firmware specifications

Firmware v1.8x



CJS Technology Limited

Date 23rd June 2006

Page 9 of 16

M x Defines the key strategy Mode (for Mifare cards). This defines the keysets to use when reading from and writing to a card. X is supplied as follows:

0 - Each of the first 8 keysets (0-7) is tried in turn until a match is found and the operation succeeds, or the keysets run out and the operation fails.

1 – The keyset relevant to the sector involved is tried. Sector 0 uses key 0, sector 3 uses key 3 etc.

2 – The Dynamic keyset is used. See the D command for details.

Send Example

ASCII

>M 02<CR>

Binary

STX	LEN	CMD	P1	CSUM	ETX
0x02	0x02	0x4D	0x02	0x4F	0x03

Return Example

ASCII

00 00 <CR>

Binary

STX	RES	LEN	CSUM	ETX
0x02	0x00	0x00	0x00	0x03

Note that the Mode value is stored in non-volatile memory. To avoid premature failure of the non-volatile memory, do not make frequent changes to the Mode value. However, issuing a Mode command which has the same value as the previous Mode value does not result in a write to the non-volatile memory. It is therefore acceptable to set a Mode value as part of the reader initialisation by your host software.

There does not need to be a card on the reader for this command to be used.

See also commands D (the Dynamic Key command), K (the Key command) and A (the key Access conditions command).

Diamond 650 Card Reader firmware specifications

Firmware v1.8x



CJS Technology Limited

Date 23rd June 2006

Page 10 of 16

R x Reads a block of card memory and returns the contents.
X Up to 4 digits of block number in hexadecimal (note - 2 bytes in binary mode).

The reader will read 16 bytes of the card memory starting at block X

Send Example

ASCII

>R 02<CR>

Binary

STX	LEN	CMD	P1	CSUM	ETX
0x02	0x03	0x52	0x00 0x02	0x50	0x03

Return example

Ascii - a string of hex values represented as two ASCII digits separated by space characters, eg:
00 10 FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF

Binary – a string of hex values., eg

STX	RES	LEN					CSUM	ETX
0x02	0x00	0x10						
RD							CSUM	ETX
0xFF 0xFF 0xFF 0xFF 0xFF 0xFF 0xFF 0xFF 0xFF 0xFF 0xFF 0xFF 0xFF 0xFF 0xFF 0xFF							0x10	0x03

Note that for Mifare Classic and 4K cards, 16 bytes represents one block. For a SuperLight card which has a block length of 4 bytes, 16 bytes will be returned regardless. The first 4 bytes will be the contents of the requested block X. The following 12 bytes will be the contents of blocks X+1, X+2 and X+3. The Innovision Jewel card is byte-addressed, and will return 16 bytes starting at the specified byte location. Note that a Read command which tries to retrieve data beyond the end of a card's physical memory will wrap back to address 0 and return data from the beginning of the card memory. Eg, reading an Ultralight from block 14 (R 0E) will return the 16 bytes from blocks 14, 15, 0 and 1.

Error Codes

- 0 - Success
 - 2 - Command timeout failure (binary mode only)
 - 3 - Command checksum failure or no ETX(binary mode only)
 - 4 - Unrecognised command
- Other values – Card removed or key Access conditions / keys unacceptable

The V command must be issued at some stage prior to issuing this command for the current card.

Diamond 650 Card Reader firmware specifications

Firmware v1.8x

Date 23rd June 2006
Page 11 of 16



T x Defines the reader terminal (or ID) number.
X Ascii - up to 4 digit hex value. Binary – a 2 byte integer.

Send Example

ASCII
>**T 1234** <CR>

Binary

STX	LEN	CMD	P1	CSUM	ETX
0x02	0x03	0x54	0x12 0x34	0x72	0x03

Return Example

ASCII
00 02 12 34 <CR>

Binary

STX	RES	LEN	RD	CSUM	ETX
0x02	0x00	0x02	0x12 0x34	0x24	0x03

If your scheme requires transactions to be tagged with the unique identity of the reader from which they originated, you may specify a unique tag or ID for this reader using this command.

There does not need to be a card on the reader for this command to be used.

See also the I command.

Diamond 650 Card Reader firmware specifications

Firmware v1.8x



CJS Technology Limited

Date 23rd June 2006

Page 12 of 16

V Verify card. This command checks for the presence of a card on the reader, and must be issued at least once before the Read or Write commands can be used. The card type, followed by the card serial number are returned if a card is present. The continued presence of a card can be established by polling using the **V** command.

Send Example

ASCII

>V <CR>

Binary

STX	LEN	CMD	CSUM	ETX
0x02	0x01	0x56	0x56	0x03

Return Example

ASCII

00 05 01 E1 B5 D2 C1<CR>

Binary

STX	RES	LEN	RD	CSUM	ETX
0x02	0x00	0x05	0x01 0xE1 0xB5 0xD2 0xC1	0x42	0x03

The first byte of the response denotes the card type. Currently these are:

TypeA/Superlight	0x00
Jewel	0x02
Mifare Classic 1K	0x08
Mifare 4K	0x18
Lite	0x01
Desfire	0x20
JCOP	0x28

Returns:

- 00 – Success
- 02 - Command timeout failure (binary mode only)
- 03 – Command checksum failure or no ETX (binary mode only)
- Other values - The card has been removed or is not present

Notes:

- Different card types return different length serial numbers.
- Once selected using the ‘V’ command, the Jewel card will respond with a failure if still present when a further ‘V’ command is issued. If you are polling to establish the removal of the card from the reader, issue two V commands at a time and consider the card to be still present until both ‘V’ commands fail. Other cards do not behave in this manner.

Diamond 650 Card Reader firmware specifications

Firmware v1.8x



CJS Technology Limited

Date 23rd June 2006

Page 13 of 16

W x y Writes a block of data to the card.

X Up to 4 digits of start address in hexadecimal (note - 2 bytes in binary mode).

Y A string of 2 digit hex values denoting the values to be written.

Send Example

ASCII

>W 02 11 22 33 44 55 66 77 88 99 AA BB CC DD EE FF 00<CR>

Binary

STX	LEN	CMD	P1								CSUM	ETX					
0x02	0x13	0x57	0x00	0x02													
P2																	
0x11	0x22	0x33	0x44	0x55	0x66	0x77	0x88	0x99	0xAA	0xBB	0xCC	0xDD	0xEE	0xFF	0x00	0x55	0x03

Returns

ASCII

00 00 <CR>

Binary

STX	RES	LEN	CSUM	ETX
0x02	0x00	0x00	0x00	0x03

For Mifare Classic and 4K cards, Y must be 16 bytes (32 chars in ASCII mode), this being the block length. For SuperLite cards, the block length is only 4 bytes. However, the Write command will accept 4, 8, 12 or 16 bytes for writing to these cards, and will write blocks X, X+1, X+2 and X+3 with the data. Eg, the command:

W 3 00112233445566778899AABBCCDDEEFF

Will write

00 11 22 33 to block 3

44 55 66 77 to block 4

88 99 AA BB to block 5

CC DD EE FF to block 6

An Innovision Jewel has an effective block length of 1 byte, and will accept between 1 and 16 bytes of data from each Write command.

Writing beyond the end of a card's physical memory will probably fail.

The V command must be issued at some stage prior to issuing this command for the current card.

Error Codes

- 0 - Success
- 2 - Command timeout failure (binary mode only)
- 3 - Command checksum failure or no ETX (binary mode only)
- 4 - Unrecognised command
- 5 - Parameter error

Other values – Card removed or key Access conditions / keys unacceptable

© CJS Technology Limited

48 Coton Park Drive, Rugby, CV23 0WN

Tel: +44 (0)8700 170660 • Email: enquiries@cjstechnology.com • Website: www.cjstechnology.com

Registered in England: Number 04896183

Diamond 650 Card Reader firmware specifications

Firmware v1.8x

Date 23rd June 2006
Page 14 of 16



Appendix 1 - Starting from scratch

Run a terminal emulator set to 115200 baud , no parity, 8 data, 1 stop bit.

If using ASCII commands via a terminal emulator, ensure the following settings are observed:

Emulation: ANSIW
Backspace key sends: Ctrl H, Space, Ctrl H
Baud Rate: 115200, n, 8, 1
Flow control: None

If you have correctly set up the terminal emulator, pressing <Return> should cause the reader to respond with:

```
04 00  
>
```

Power cycle the reader for the boot message

Diamond v<VER> ID.<ID> S<ST>

If required, change the baud rate using the B command. Adjust the terminal software to suit.

Set some keysets as follows:

```
K 0 FFFFFFFFFFFFFFFFFFFFFFFFFF <Return> (a zero followed by 24 F characters)  
K 1 A0A1A2A3A4A5B0B1B2B3B4B5 <Return>
```

The unit will default to key Mode 0, which allows the reader to choose the keyset. Key Access conditions will default to 4, which allows the reader to choose key A or Key B for reading and writing. This should be sufficient to enable a blank mifare card to be used with the reader.

Diamond 650 Card Reader firmware specifications

Firmware v1.8x

Date 23rd June 2006
Page 15 of 16



Now place a blank Mifare card on the reader and issue the Verify command:

V<Return>

The reader should respond with something like:

00 05 08 xx xx xx xx

The first return parameter is **00** indicating success. The **05** denotes that there are 5 bytes of response to follow. **08** indicates a Mifare Classic card, and the 4 bytes shown here as 'xx' will be the card serial number for this particular card.

You should now be able to read from a block on the card. Enter the Read command:

R 04<Return>

This reads block 4, which is the first block of sector 1. Assuming that the keys provided are suitable, the reader will respond with something like:

00 10 xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx

The first return parameter is **00** indicating success. The **10** tells us that there are 16 bytes of response to follow. The 16 bytes shown here as 'xx' will be the data retrieved from block 4 of this particular card.

You should now be able to write to a block on the card. Enter the Write command:

W 04 0102030405060708090A0B0C0D0E0F10<Return>

This will write to the 16 bytes in block 4, which is the first block of sector 1. Assuming that the keys provided are suitable, the reader will respond with:

00 00

The first return parameter is **00** indicating success. The second **00** tells us that there are no further bytes of response to follow.

Diamond 650 Card Reader firmware specifications Firmware v1.8x

Date 23rd June 2006
Page 16 of 16



Another Read of block 4

R 04<Return>

should return:

00 10 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F 10

Notes:

- If the card is removed from the reader at any stage, it will be necessary to issue the V command again before using the Read or Write commands.
- In the event that a glitch or power-outage causes the reader to reset, it will immediately send the following bytes to the host.

<STX><0xFF><0x00><0xFF><ETX><0x0C>
followed by the ascii startup string

The host must be prepared to accept this information at any time and be able to respond by:

Aborting whatever command may have been in progress,
Resetting the Dynamic Key (D command - if dynamic keys are in use),
Resetting the Key Access conditions (A command - if these are in use), and
Re-establishing communications with the card using a V command.

- In the event that you accidentally send badly formed or corrupted data to the reader, it is possible that the reader will interpret data as commands. This is particularly likely when using the ASCII interface which does not have checksum and data length protection. This may result in non-volatile parameters becoming overwritten. Non-volatile parameters are as follows:

Keysets	(K command)
Key mode	(M command)
Terminal ID	(T command)