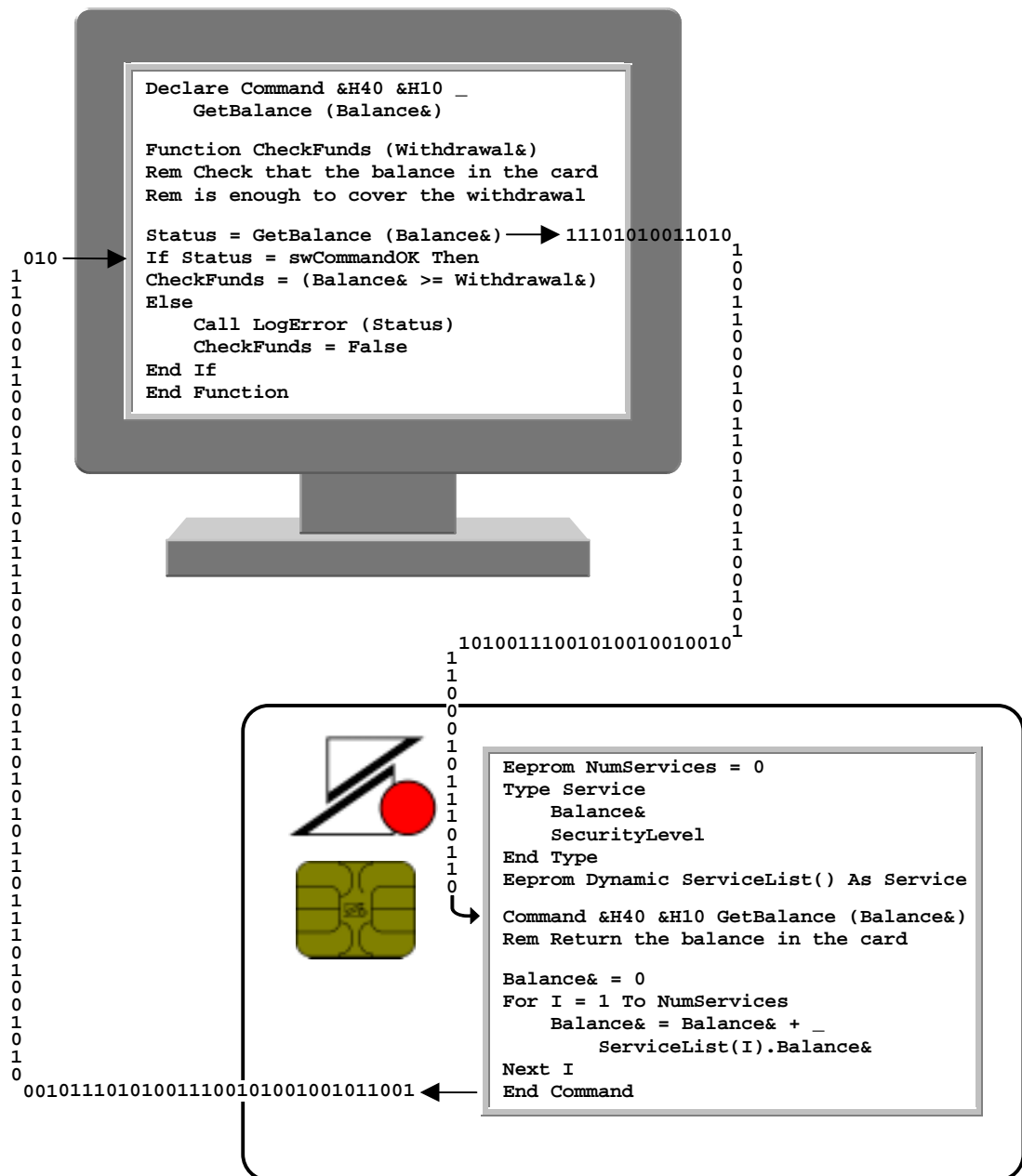


BasicCard



The Compact, Enhanced, and Professional BasicCards

The ZeitControl BasicCard Family

The Compact, Enhanced, and Professional BasicCards

Document version 4.50

19th April 2003

Author: Tony Guilfoyle

e-mail: development@ZeitControl.de

Copyright© ZeitControl cardsystems GmbH
Siedlerweg 39
D-32429 Minden
Germany

Tel: +49 (0) 571-50522-0

Fax: +49 (0) 571-50522-99

Web sites:

<http://www.ZeitControl.de>

<http://www.BasicCard.com>

Overview

Like most computer hardware, the price of smart cards is steadily decreasing, while performance and capacity are improving all the time. You can now buy a fully-functional computer, the size of your thumb-nail, for just a euro or two. However, before the BasicCard arrived, the cost of developing software for smart cards was out of all proportion to the cost of the hardware. A typical development project might take six months and cost a quarter of a million euros. This was a major barrier to the widespread use and acceptance of smart cards.

But now you can program your own smart card in an afternoon, with no previous experience required. If you can program in Basic, you can design and implement a custom smart card application. With ZeitControl's BasicCard, the development cycle of writing code, downloading, and testing takes a few minutes instead of weeks.

This document describes ZeitControl's BasicCard family: the Compact BasicCard, the Enhanced BasicCard, and the Professional BasicCard. A BasicCard contains 256-1686 bytes of RAM, and 1-31 kilobytes of user-programmable EEPROM. The EEPROM contains the user's Basic code, compiled into a virtual machine language known as P-Code (the Java programming language uses the same technology). The user's permanent data is also stored in EEPROM, either as Basic variables, or in the BasicCard's directory-based file system. The RAM contains run-time data and the P-Code stack.

The smallest BasicCard, the Compact BasicCard, contains 1 kilobyte of EEPROM. How much Basic code can you squeeze into this card? While no exact figure can be given, our experience suggests a ratio of about 10-20 bytes of P-Code to every statement of Basic code. Assuming on average one statement every two lines (for comments and blank lines), this works out at 100-200 lines of source code. And the Series 4 Professional BasicCards can hold 30 times as much.

To create P-Code and download it to the BasicCard, you need ZeitControl's BasicCard support software. This software is *free of charge*, and can be downloaded at any time from ZeitControl's BasicCard page on the Internet (www.BasicCard.com). The support software runs under Microsoft® Windows® 98/NT/2000. With this support package, you can test your software even if you don't have a card reader, by simulating the BasicCard in the PC. The package contains a fully-functional Multiple Debugger, that can run Terminal and BasicCard programs simultaneously. So you can try out your idea for a smart card application without it costing you a cent.

The Smart Card Environment

Obviously, programming a smart card is not the same as programming a desktop computer. It has no keyboard or screen, for a start. So how does a smart card receive its input and communicate its output? It talks to the outside world through its bi-directional I/O contact. Communication takes place at 9600 baud or more, according to the T=0 and T=1 protocols defined in ISO/IEC standards 7816-3 and 7816-4. But this is completely invisible to the Basic programmer – all you have to do is define a command in the card, and program it like an ordinary Basic procedure. Then you can call this command from a ZC-Basic program running on the PC. Again, the command is called as if it was an ordinary procedure.

The BasicCard operating system takes care of all the communications for you. It will even encrypt and decrypt the commands and responses if you ask it to. All you have to do is specify a different two-byte ID for each command that you define. (If you are familiar with **ISO/IEC 7816-4: Interindustry commands for interchange**, you will know these two bytes as **CLA** and **INS**, for Class and Instruction.)

Here is a simple example. Suppose you run a discount warehouse, and you are issuing the BasicCard to members to store pre-paid credits. You will want a command that returns the number of credits left in the card. So you might define the command GetCustomerCredits, and give it an ID of &H20 &H02 (&H is the hexadecimal prefix):


```

Eeprom CustomerCredits ' Declare a permanent Integer variable
Command &H20 &H02 GetCustomerCredits (Credits)
    Credits = CustomerCredits
End Command

```

You can call this command from the PC with the following code:

```

Const swCommandOK = &H9000
Declare Command &H20 &H02 GetCustomerCredits (Credits)
Status = GetCustomerCredits (Credits)
If Status <> swCommandOK Then GoTo CancelTransaction

```

The value &H9000 is defined in **ISO/IEC 7816-4** as the status code for a successful command. This value is automatically returned to the caller unless the ZC-Basic code specifies otherwise. The return value from a command should always be checked, even if the command itself has no error conditions – for instance, the card may have been removed from the reader.

It's as simple as that. Of course, there is a lot more going on below the surface, but you don't have to know about it to write a BasicCard application.

Technical Summary

All BasicCard families (Compact, Enhanced, and Professional) contain:

- a full implementation of the **T=1** block-level communications protocol defined in **ISO/IEC 7816-3: *Electronic signals and transmission protocols***, including chaining, retries, and WTX requests;
- a command dispatcher built around the structures defined in **ISO/IEC 7816-4: *Interindustry commands for interchange (CLA INS P1 P2 [Lc IDATA] [Le])***;
- built-in commands for loading EEPROM, enabling encryption, etc.;
- a Virtual Machine for the execution of ZeitControl's P-Code;
- code for the automatic encryption and decryption of commands and responses, using the **AES**, **DES**, or **SG-LFSR** symmetric-key algorithm.

Enhanced and Professional BasicCards contain in addition:

- a directory-based, DOS-like file system;
- IEEE-compatible floating-point arithmetic.

The functionality of the Enhanced BasicCard family can be further extended using Plug-In Libraries.

Professional BasicCards contain in addition:

- a Public-Key algorithm (**RSA** or **EC**);
- a full implementation of the **T=0** byte-level communications protocol defined in **ISO/IEC 7816-3: *Electronic signals and transmission protocols***;
- the **SHA-1** Secure Hash Algorithm.

The data sheet on the next page contains details of available BasicCards versions, and the cryptographic algorithms that they support.

Development Software

The **ZeitControl MultiDebugger** software support package consists of:

- **ZCPDE**, the Professional Development Environment;
- **ZCMDTERM** and **ZCMDCARD**, debuggers for Terminal programs and BasicCard programs;
- **ZCMBASIC**, the compiler for the ZC-Basic language;
- **ZCMSIM**, for low-level simulation of Terminal and BasicCard programs;
- **BCLOAD**, for downloading P-Code to the BasicCard;
- **KEYGEN**, a program that generates random keys for use in encryption;
- **BCKEYS**, for downloading cryptographic keys to the Compact and Enhanced BasicCards.

Compact BasicCard

Version	EEPROM	RAM	Protocol	Encryption	Floating-Point Support	File System
ZC1.1	1K	256 bytes	T=1	SG-LFSR	None	No

Enhanced BasicCard

Version	EEPROM	RAM	Protocol	Encryption	Extras	FP Support	File System
ZC3.1	2K	256 bytes	T=1	DES		Full	Yes
ZC3.2	4K	256 bytes	T=1	DES		Full	Yes
ZC3.3	8K	256 bytes	T=1	DES		Full	Yes
ZC3.4	16K	256 bytes	T=1	DES		Full	Yes
ZC3.5	6K	256 bytes	T=1	DES	EC-FSA¹	Full	Yes
ZC3.6	14K	256 bytes	T=1	DES	EC-FSA¹	Full	Yes
ZC3.7	2K	256 bytes	T=1	DES		Full	Yes
ZC3.8	4K	256 bytes	T=1	DES		Full	Yes
ZC3.9	8K	256 bytes	T=1	DES		Full	Yes

¹ EC-FSA: Fast Signature Algorithm for Elliptic Curve Cryptography

Plug-In Libraries for the Enhanced BasicCard: **EC-161, AES, SHA-1, IDEA**

Professional BasicCard¹

Version	PK Algorithm	EEPROM	RAM	Protocol	Encryption	Extras	FP Support	File System
ZC4.5A	RSA	30K	1K	T=0, T=1	AES	SHA-1	Partial²	Yes
ZC4.5D	RSA	30K	1K	T=0, T=1	DES	SHA-1	Partial²	Yes
ZC5.4	EC-167	16K	1K	T=0, T=1	AES & DES	SHA-1	Full	Yes
ZC5.5	EC-167	31K	2K	T=0, T=1	AES & DES	SHA-1	Full	Yes

¹ See **Professional BasicCard Datasheet** for more information

² Single-to-String conversion not supported

Public-Key Algorithms

Name	Description	Key size	Reference
RSA	Rivest-Shamir-Adleman algorithm	1024 bits	IEEE P1363: Standard
EC-167	Elliptic Curve Cryptography over the field $GF(2^{167})$	167 bits	Specifications for Public
EC-161	Elliptic Curve Cryptography over the field $GF(2^{168})$	161 bits	Key Cryptography

Symmetric-Key Algorithms

Name	Description	Key size	Reference
AES	Advanced Encryption Standard	128/192/ 256 bits	Federal Information Processing Standard FIPS 197
DES	Data Encryption Standard	56/112 bits	ANSI X3.92-1981: Data Encryption Algorithm
SG-LFSR	Shrinking Generator – Linear Feedback Shift Register	64 bits	D. Coppersmith, H. Krawczyk, and Y. Mansour, The Shrinking Generator, Advances in Cryptology – CRYPTO '93 Proceedings, Springer-Verlag, 1994
IDEA	International Data Encryption Algorithm	128 bits	X. Lai, On the Design and Security of Block Ciphers, ETH Series in Information Processing, v. 1, Konstanz: Hartung-Gorre Verlag, 1992

Data Hashing Algorithms

Name	Description	Reference
SHA-1	Secure Hash Algorithm, revision 1	Federal Information Processing Standard FIPS 180-1

Communication Protocols

Name	Description	Reference
T=0	Byte-level transmission protocol	ISO/IEC 7816-3: Electronic signals and transmission protocols
T=1	Block-level transmission protocol	

Contents

Part I: User's Guide

1. The BasicCard	6
1.1 Processor Cards	6
1.2 Programmable Processor Cards	7
1.3 BasicCard Features	8
1.4 BasicCard Programs	9
1.5 BasicCard Program Layout	9
1.6 The Compact BasicCard	11
1.7 The Enhanced BasicCard	11
1.8 The Professional BasicCard	12
2. The Terminal	13
2.1 The Terminal Program	13
2.2 Terminal Program Layout	13
3. The ZC-Basic Language	16
3.1 The Source File	16
3.2 Tokens	16
3.3 Pre-Processor Directives	18
3.4 Data Storage	21
3.5 Data Types	22
3.6 Arrays	22
3.7 Data Declaration	23
3.8 User-Defined Types	24
3.9 Expressions	25
3.10 Assignment Statements	27
3.11 Program Control	28
3.12 Procedure Definition	31
3.13 Procedure Declaration	33
3.14 Procedure Calls	35
3.15 Procedure Parameters	36
3.16 Built-in Functions	37
3.17 Encryption	39
3.18 Random Number Generation	42
3.19 Error Handling	42
3.20 BasicCard-Specific Features	43
3.21 Terminal-Specific Features	44
3.22 Miscellaneous Features	48
3.23 Technical Notes	49

4. Files and Directories	51
4.1 Directory-Based File Systems	51
4.2 The BasicCard File System	52
4.3 File System Commands	53
4.4 Directory Commands	54
4.5 Creating and Deleting Files	58
4.6 Opening and Closing Files	58
4.7 Writing To Files	60
4.8 Reading From Files	61
4.9 File Locking and Unlocking	62
4.10 Miscellaneous File Operations	64
4.11 File Definition Sections	64
4.12 The Definition File FILEIO.DEF	65
5. Support Software	67
5.1 Hardware Requirements	67
5.2 Installation	67
5.3 File Types	67
5.4 Physical and Virtual Card Readers	69
5.5 Windows-Based Software	69
5.6 The ZCPDE Professional Development Environment	71
5.7 The ZCMDTERM Terminal Program Debugger	73
5.8 The ZCMDCARD BasicCard Program Debugger	75
5.9 Command-Line Software	77
6. Plug-In Libraries	83
6.1 RSA: The Rivest-Shamir-Adleman Library	83
6.2 AES: The Advanced Encryption Standard Library	87
6.3 EC-167: The 167-Bit Elliptic Curve Library	88
6.4 EC-161: The 161-Bit Elliptic Curve Library	92
6.5 SHA-1: The Secure Hash Algorithm Library	97
6.6 IDEA: International Data Encryption Algorithm	98
6.7 MATH: Mathematical Functions	99
6.8 MISC: Miscellaneous Procedures	100

Part II: Technical Reference

7. Communications	106
7.1 Overview	106
7.2 Answer To Reset	106
7.3 The T=0 Protocol	107
7.4 The T=1 Protocol	112
7.5 Commands and Responses	113
7.6 Status Bytes SW1 and SW2	114
7.7 Pre-Defined Commands	117
7.8 The Command Definition File COMMANDS.DEF	134
8. Encryption Algorithms	137
8.1 The DES Algorithm	137
8.2 Implementation of DES in the BasicCard	138
8.3 Certificate Generation Using DES	142
8.4 The AES Algorithm	142
8.5 Implementation of AES in the Professional BasicCard	142
8.6 The SG-LFSR Algorithm	145
8.7 Implementation of SG-LFSR in the Compact BasicCard	145
8.8 SG-LFSR with CRC	146
8.9 Encryption – a Worked Example	147
9. The ZC-Basic Virtual Machine	155
9.1 The BasicCard Virtual Machine	155
9.2 The Terminal Virtual Machine	155
9.3 The P-Code Stack	156
9.4 Run-Time Memory Allocation	157
9.5 Data Types	157
9.6 P-Code Instructions	158
9.7 The SYSTEM Instruction	164
10. Output File Formats	168
10.1 ZeitControl Image File Format	168
10.2 ZeitControl Debug File Format	171
10.3 List File Format	174
10.4 Map File Format	176
Index	178

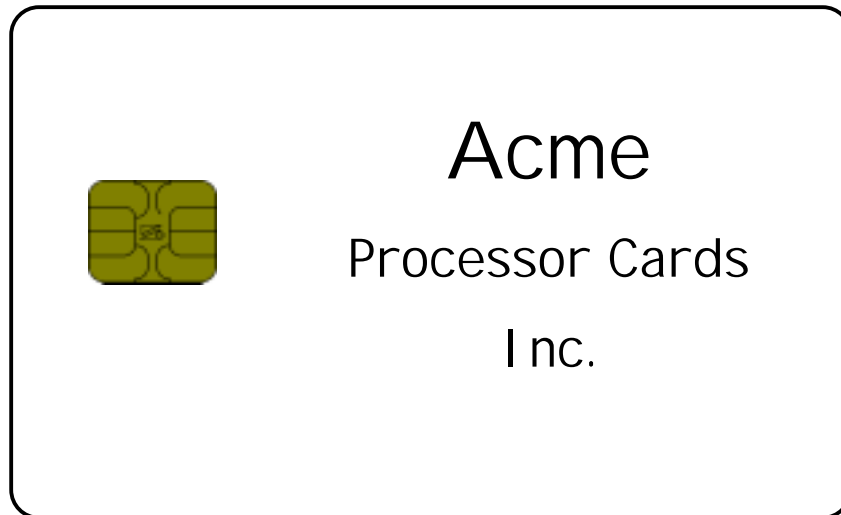
Part I

User's Guide

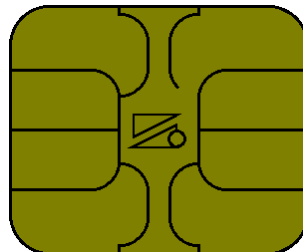
1. The BasicCard

1.1 Processor Cards

A processor card looks like this:



Most of this is just plastic. The important part is the metallic contact area:

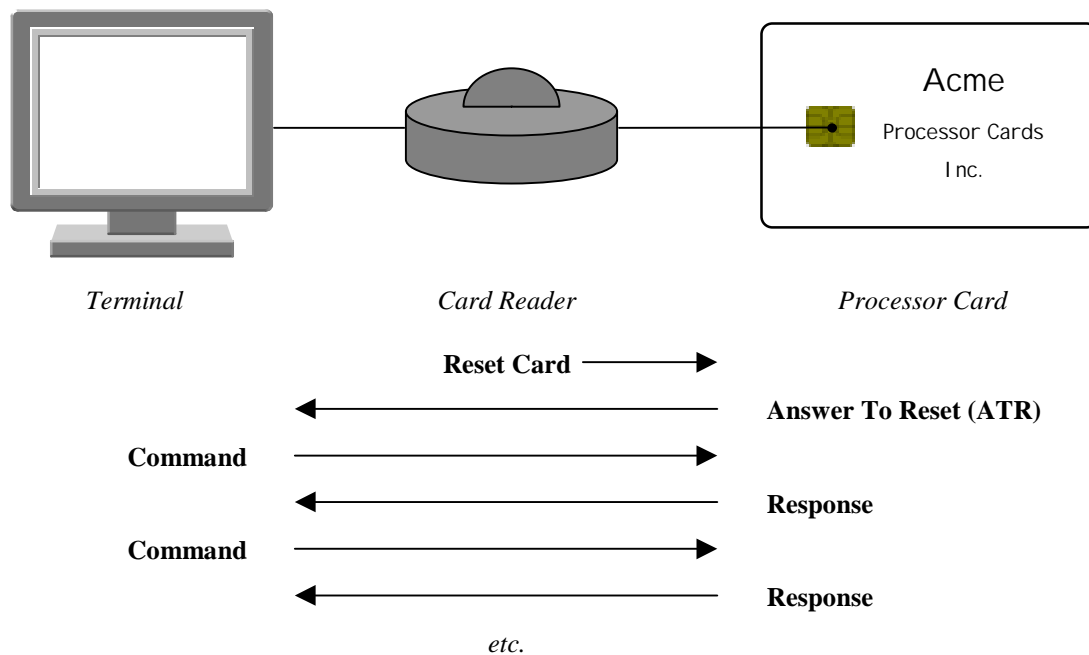


This area has the same layout as a standard telephone card. However, a telephone card contains only memory, while a processor card contains a CPU as well – in effect, a complete miniature computer. A typical processor card today might contain 8-32 kilobytes of ROM (Read-Only Memory) for the operating system machine code, 1-64 kilobytes of EEPROM (Electrically Erasable, Programmable Read-Only Memory) for the data in the card, and 256-2048 bytes of RAM (Random Access Memory). The EEPROM is the ‘hard disk’ of the card – data written to EEPROM retains its value when the card is powered down.

The single most important aspect of processor card design is security. That’s what processor cards are for. If I want to make telephone calls for free, I can buy the equipment to make my own telephone cards – but the reward is not proportional to the effort required (not to mention the risk of detection). But if those telephone cards contained real money, instead of just telephone credits, there would be plenty of people working on making illegal copies.

So for cards that contain so-called *electronic cash* that can be spent like real money, a processor card is required. The processor protects access to the memory, using tamper-proof hardware design coupled with high-security software algorithms.

Communication with a processor card is by means of a *command-response* protocol. When a card is inserted in the reader, a command-response session is initiated:



The processor card is the passive partner in this exchange. After sending the Answer To Reset, it does nothing until it receives a command from the Terminal. Then after sending the response to this command, it waits passively for the next command, and so on. The command-response protocol used by most processor cards is defined in the **ISO** standard documents **ISO/IEC 7816-3: Electronic signals and transmission protocols** and **ISO/IEC 7816-4: Interindustry commands for interchange**. These documents are summarised in **Chapter 7: Communications**.

1.2 Programmable Processor Cards

Until recently, programming a processor card was a major undertaking. The following skills were involved:

- Assembly language programming. Although 'C' compilers were available for some processor cards, it was not possible to write the whole operating system in 'C'.
- Byte-level communication protocols, such as the **T=0** protocol.
- Block-level communication protocols at the command-response level.
- Programming at the hardware level for writing to EEPROM.
- Security algorithms. You had to write your own.

You would also need a complex (and expensive) development environment. And on top of everything, after submitting your program to the chip manufacturer, you would have to wait for two or three months, while it was burned into ROM in several thousand chips, before you could test it in a real card.

However, the situation has improved. Programmable processor cards are now available. The heart of a programmable processor card is its P-Code interpreter. You write a program for the card, in Java or Basic (the two languages currently available on the market). This is compiled into so-called P-Code, which is a machine-independent language that looks like machine code. The P-Code is downloaded to the card, where it is executed by the interpreter. And if your code doesn't work first time, you can download a new version into the same card. So the development cycle is closer to what most programmers are used to.

1. The BasicCard

1.3 BasicCard Features

The BasicCard is a programmable processor card, with a P-Code interpreter optimised for executing programs written in Basic. It was designed with four criteria in mind at all times. It had to be:

Inexpensive The development software is *free of charge* – you can download the latest version from our web site at any time at www.BasicCard.com. And most versions of the BasicCard cost less than half as much as other currently-available programmable processor cards.

Easy to program Everybody can program in Basic – or if they can't, they can pick it up in an afternoon. That's all you need to program the BasicCard. A command from the Terminal to the BasicCard is defined and called just like a Basic function. The file system in the BasicCard looks just like a regular diskette. Encryption has been made as simple as possible to implement – you just turn it on or off. And EEPROM data is read and written just like RAM data.

Secure State-of-the-art cryptographic algorithms are available for all BasicCard types:

Professional BasicCard

- public-key cryptography: **RSA**, or **EC** over $GF(2^{167})$
- the **AES** Advanced Encryption Standard
- the **SHA-1** Secure Hash Algorithm

Enhanced BasicCard

- **DES** Data Encryption Standard
- Plug-In Libraries: **AES**, **SHA-1**, **EC** over $GF(2^{168})$, and the **IDEA** International Data Encryption Algorithm

Compact BasicCard

- the Shrinking Generator algorithm designed by D. Coppersmith, H. Krawczyk, and Y. Mansour – see **8.6 The SG-LFSR Algorithm** for details

The security of the BasicCard implementation is enhanced by our cryptographic key generation program – see **5.9.4 The Key Generator KEYGEN.EXE** for more information.

ISO-compliant In the ZC-Basic programming language, defining your own **ISO**-compliant command is as easy as declaring a function. Just as importantly, **ISO**-defined commands, such as **SELECT FILE** and **READ RECORD**, can be programmed in ZC-Basic. So you can implement your own **ISO** card, or call an existing **ISO** card from a ZC-Basic Terminal program. See **7.5 Commands and Responses** for more information.

The operating systems in all BasicCards contain the following features:

- A full implementation of the **T=1** communications protocol defined in **ISO/IEC 7816-3: Electronic signals and transmission protocols**, including chaining, retries, and WTX requests. The Professional BasicCards contain the **T=0** protocol as well.

These protocols define the structure and duration of the bits and bytes that constitute the messages in a command-response session. See **7.3 The T=0 Protocol** and **7.4 The T=1 Protocol** for more information.

- Pre-defined commands for downloading programs and data to the BasicCard, enabling automatic encryption, etc.

These commands are described in **7.7 Pre-Defined Commands**.

- A Virtual Machine for the execution of ZeitControl's P-Code.

The compiler **ZCMBASIC** compiles ZC-Basic source code into P-Code, an intermediate language that can be thought of as the machine code for a Virtual Machine. (The Java programming language uses the same technology, although the P-Code instruction set is not the same.) The P-Code is downloaded to the card using the **BCLOAD** Card Loader program. Then the Virtual Machine in the BasicCard executes the P-Code instructions at run-time.

1.4 BasicCard Programs

BasicCard programs are written in the ZC-Basic language, which is a modern procedure-oriented Basic, with special features for the processor card environment. It is described in **Chapter 3: The ZC-Basic Language**.

A BasicCard program is specified in a single source file (which may, however, include other source files). This file will typically have a **.BAS** extension.

1.4.1 Image Files

The compiler can create a ZeitControl Image File (with **.IMG** extension) from your BasicCard program source file. This image file can then be downloaded to a BasicCard; or it can be run in the **ZCMSIM** P-Code interpreter together with a Terminal Program – see **5.9.2 The P-Code Interpreter ZCMSIM.EXE** for details.

1.4.2 Debug Files

If the BasicCard program is to be run in the **ZCMD CARD** BasicCard debugger, the compiler must create a ZeitControl Debug File (with **.DBG** extension). This is simply a ZeitControl Image File with symbolic debugging information included. Image files and debug files are described in **Chapter 10: Output File Formats**.

1.4.3 Card Program Files

The **ZCMD CARD** BasicCard debugger works with simulated BasicCards. A simulated card is described by a Card Program File, with extension **.ZCC**. This file contains the simulated EEPROM, which retains its contents between program runs, and various other data, such as source filename, card type, and compiler options. A single source file may be the basis for several Card Program files, each running the same program, but with different data stored in simulated EEPROM.

1.5 BasicCard Program Layout

A BasicCard program consists of *initialisation code* and *procedure definitions*. Programs for the Enhanced and Professional BasicCards can also contain optional *file definition sections*.

1.5.1 Initialisation Code

The first block of code that is not contained inside a procedure definition is *initialisation code*: it gets executed when the first user-defined command is called from the Terminal. Initialisation code is not required, but it can be useful for certain things; for instance, checking that the card has not been cancelled by the issuer, or that the expected files and directories are present.

1.5.2 Procedure Definitions

ZC-Basic has three types of procedure: subroutines, functions, and commands. Each procedure is self-contained – nested procedure definitions are not allowed, and **GoTo** and **GoSub** statements can only transfer control to labels within the current procedure. Subroutines and functions are familiar to Basic programmers – a subroutine is a block of code that can be called from other procedures, and a function is a subroutine that returns a value. The command, however, is special to ZC-Basic; it is the mechanism by which the Terminal program communicates with the BasicCard program.

According to the **ISO** standard document **ISO/IEC 7816-4: Interindustry commands for interchange**, each command is assigned a unique two-byte ID. This is all the ZC-Basic programmer needs to know about ISO standards. For the curious, these two bytes are known as **CLA** and **INS** (for Class and Instruction); the full command-response protocol defined in the standard is described in **7.5 Commands and Responses**. The two-byte ID must be supplied between the **Command** keyword and the name of the command. Here is an example (&H is the hexadecimal prefix):

1. The BasicCard

```
Command &H80 &H10 GetCustomerName (Name$)
    Name$ = CustomerName$
End Command
```

Then whenever the BasicCard receives a command from the Terminal with **CLA = &H80** and **INS = &H10**, the operating system in the card automatically executes the **GetCustomerName** command.

A command behaves like a cross between a function and a subroutine: it is defined like a subroutine (as above), but called like a function (see **2.2 Terminal Program Layout**). The BasicCard operating system fills in the return value that gets passed back to the Terminal program. This return value consists of the two status bytes **SW1** and **SW2** defined in **ISO/IEC 7816-4**. The return value of a command should always be checked; for instance, the card may have been removed from the reader, or the reader may have lost power for some reason. If **SW1 = &H90** and **SW2 = &H00**, or if **SW1 = &H61**, then the command completed successfully. Otherwise a problem has occurred that prevented successful execution of the command.

These two status bytes are available as pre-defined variables in the BasicCard, so you can define your own error codes. For convenience of access, the two-byte **Integer** variable **SW1SW2** is also defined. For instance:

```
Eeprom Balance As Long : Rem Declare permanent (Eeprom) variable
Const InsufficientCredit = &H6F00
Command &H80 &H20 DebitAccount (Amount As Long)
    If Balance < Amount Then
        SW1SW2 = InsufficientCredit
    Else
        Balance = Balance - Amount
    End If
End Command
```

Notes:

- You don't need to specify **SW1** and **SW2** if the command completes successfully. They are set to **&H90** and **&H00** before the command is called.
- If you specify values for **SW1** and **SW2** other than the two indicators of successful completion (**SW1SW2 = &H9000** or **SW1 = &H61**), the operating system throws away the response data and just returns the two status bytes to the Terminal program. (This is in accordance with **ISO/IEC 7816-4**.) In the Professional BasicCard, you can override this behaviour – see **3.3.3 Options** and **6.8.8 SW1-SW2 Processing** for details.
- Your own **SW1-SW2** error codes can take any values. However, for **ISO** compliance, or if you are programming a Professional BasicCard that uses the **T=0** protocol, the high nibble of **SW1** must be **6**, i.e. **SW1 = &H6X**. You should also avoid assigning new meanings to ZC-Basic's own error codes. ZC-Basic's error codes are listed in **7.6 Status Bytes SW1 and SW2**; you can avoid any clashes if you use **SW1 = &H6B** or **&H6F** (except **SW1-SW2=&H6F00**).

1.5.3 File Definition Sections

The Enhanced and Professional BasicCards contain a Windows-like file system, with directories organised in a tree structure. There are several ways to access files and directories in the BasicCard.

- From within the BasicCard itself, files can be created, read, and written with exactly the same statements that you would use in a Basic program running under DOS or Windows. There are also some special statements for setting access conditions on files and directories, to restrict access from Terminal programs. These access conditions can depend on cryptographic keys, user passwords, etc.
- From a Terminal program, the BasicCard looks just like a diskette, with the special drive name **"@:"**. If the access conditions permit it, you can create, read, and write files and directories in the BasicCard as if it was a floppy disk.
- You can initialise directory structures and files in a BasicCard program with File Definition Sections.

1.5.4 Permanent Data

Most BasicCard applications will contain permanent data, that retains its value while the BasicCard is powered down. Permanent data is stored in EEPROM (Electrically Erasable, Programmable Read-Only Memory). In the Enhanced and Professional BasicCards, you can store permanent data in files, but in the Compact BasicCard permanent data must be stored in **Eeprom** variables. An example of an **Eeprom** variable was given in the previous section:

```
Eeprom Balance As Long : Rem Declare permanent (Eeprom) variable
```

The variable **Balance** declared here can be read or written just like a regular variable. **Eeprom** strings and arrays can also be declared. This can be a very convenient way of storing permanent data, in all types of BasicCard.

Writing to EEPROM can take up to 6 milliseconds, so the possibility is always present that the card will lose power in the middle of the write operation. The Enhanced and Professional BasicCards automatically log all EEPROM write operations, to enable them to recover in the event of power loss. The Compact BasicCard has no such recovery mechanism, so EEPROM data may be left in an inconsistent state. In the Compact BasicCard, therefore, important **Eeprom** data should be duplicated to protect against possible corruption if the card is powered down during an EEPROM write operation. For example:

```
Eeprom Balance As Long : Rem A very important piece of data
Eeprom ShadowBalance As Long
Eeprom Committed = False
...
Command &H80 &H30 ChangeBalance (NewBalance As Long)
    ShadowBalance = NewBalance
    Committed = True
    Balance = ShadowBalance
    Committed = False
End Command
```

Then in the initialisation code:

```
If Committed Then
    Balance = ShadowBalance
    Committed = False
End If
```

This technique guarantees that **Balance** will never be left in an inconsistent state.

Note: In the Compact BasicCard, power loss during memory allocation can lead to corruption of the EEPROM heap. For this reason, we recommend that you avoid **ReDim** statements and assignment of variable-length strings in all Compact BasicCard code that may be executed after the card is issued to the end user. (The Enhanced and Professional BasicCards always protect themselves against heap corruption, so no such caution is necessary in these cards.)

1.6 The Compact BasicCard

A single version of the Compact BasicCard is available:

BasicCard ZC1.1 Contains 1K of user-programmable EEPROM. Available since June 1998.

1.7 The Enhanced BasicCard

The original Enhanced BasicCard – the *Series 2* Enhanced BasicCard – is no longer supported. The current Enhanced BasicCard is the *Series 3* Enhanced BasicCard:

BasicCard ZC3.1 Contains 2K of user-programmable EEPROM. Available in large quantities only – contact ZeitControl for details.

BasicCard ZC3.2 Contains 4K of user-programmable EEPROM. Available in large quantities only – contact ZeitControl for details.

1. The BasicCard

BasicCard ZC3.3	Contains 8K of user-programmable EEPROM. Available since December 1999.
BasicCard ZC3.31	Functionally identical to BasicCard ZC3.3 .
BasicCard ZC3.4	Contains 16K of user-programmable EEPROM. Available since December 1999.
BasicCard ZC3.5	Contains 6K of user-programmable EEPROM, and the Elliptic Curve Fast Signature Algorithm (EC-FSA). Available since February 2000.
BasicCard ZC3.6	Contains 14K of user-programmable EEPROM, and the Elliptic Curve Fast Signature Algorithm (EC-FSA). Available since February 2000.

The two **EC-FSA** cards contain a proprietary algorithm that can generate a 161-bit Elliptic Curve signature in 1.2 seconds.

BasicCard ZC3.7	New 2K version, equivalent to BasicCard ZC3.1 .
BasicCard ZC3.8	New 4K version, equivalent to BasicCard ZC3.2 .
BasicCard ZC3.9	New 8K version, equivalent to BasicCard ZC3.3 .

These three new versions were required due to hardware changes in the chip, but the functionality is unchanged.

1.8 The Professional BasicCard

With the arrival of the **Professional BasicCard** series, ZeitControl has revolutionised its own BasicCard development process. Two major factors have changed:

1. The BasicCard Operating System is contained in programmable Flash ROM, so that new BasicCard versions can be produced on demand, without the costly procedure of burning the code into ROM.
2. ZeitControl's MultiDebugger development software no longer needs to know the details of each BasicCard version in advance – each Professional BasicCard version comes with its own Configuration File, that contains everything that the software needs to know. So a new Professional BasicCard version can be produced without having to make any changes to the software.

All Professional BasicCards contain a built-in public-key cryptography algorithm: **ZC4.x** series cards support the **RSA** algorithm, and **ZC5.x** series cards support the **EC-167** algorithm (Elliptic Curve cryptography over the finite field $GF(2^{167})$, as defined in IEEE standard P1363).

The minor version number (the **x** in **ZC4.x** and **ZC5.x**) indicates that the amount of user-programmable EEPROM in the card is approximately 2^x kilobytes.

Currently available Professional BasicCards:

Version	User-programmable EEPROM	T=0	T=1	AES	DES	RSA	EC-167	SHA-1
ZC4.5A	30K	✓	✓	✓		✓		✓
ZC4.5D	30K	✓	✓		✓	✓		✓
ZC5.4	16K	✓	✓	✓	✓		✓	✓
ZC5.5	31K	✓	✓	✓	✓		✓	✓

From time to time, new versions of the Professional BasicCard will appear, and new features will be added to existing cards. See the **Professional BasicCard Datasheet** on ZeitControl's BasicCard web site www.BasicCard.com for the most up-to-date information.

The version number of the card, along with its software revision number, is returned by the card as an ASCII string in the response to the **GET STATE** command (see **7.7.3 The GET STATE Command**).

2. The Terminal

2.1 The Terminal Program

The ZC-Basic language was designed with the BasicCard in mind. But it can also run in a PC, with or without a card reader attached to the serial port. You can write a stand-alone ZC-Basic program to do your monthly accounts, or to help you solve crosswords, or whatever you like.

A ZC-Basic program that runs on a PC is referred to in this documentation as the **Terminal** program. Usually it will communicate with one or more ZC-Basic programs running in (real or simulated) BasicCards – the **BasicCard** programs.

The compiler can create executable files, image files, and debug files from a Terminal program source file – see **5.9.1 The ZC-Basic Compiler ZCMBASIC.EXE** for details.

2.1.1 Executable Files

The compiler can create standard executable files (files with **.EXE** extension), that will run as programs in a DOS box under Windows® 98. Such programs can't communicate with a simulated BasicCard – if they call any BasicCard commands, then a real BasicCard must be present. Also, such programs are not self-modifying, so they can't execute **Write Eeprom** statements (see **2.2.4 Permanent Data** below).

Command-line parameters passed to the executable file can be accessed from ZC-Basic in the pre-defined string array **Param\$ (1 To nParams)** – see **3.21.10 Pre-Defined Variables**.

2.1.2 Image Files

For more flexibility during program development, the compiler can also create a ZeitControl Image File (with **.IMG** extension) from your Terminal program source file. The **ZCMSIM** P-Code interpreter can then run this Terminal program together with a BasicCard program running in a real or simulated BasicCard – see **5.9.2 The P-Code Interpreter ZCMSIM.EXE** for details.

2.1.3 Debug Files

The compiler can also produce Debug Files (with **.DBG** extension), which are simply ZeitControl Image Files with debugging information included. These files are used by the **ZCMDTERM** Terminal Program debugger. Image files and debug files are described in **Chapter 10: Output File Formats**.

2.1.4 Terminal Program Files

The **ZCMDTERM** Terminal Program debugger saves the data for a given Terminal Program in a Terminal Program file, with **.ZCT** extension. This file contains the source filename, the compiler options, and various other data.

2.2 Terminal Program Layout

A Terminal program consists of the *main procedure* and *procedure definitions*. BasicCard commands are declared in *command declarations*, after which they can be called just like functions.

The Terminal program is executed by ZeitControl's P-Code interpreter, in one of three ways:

- as a stand-alone executable file (**.EXE**) created by the compiler;
- by the **ZCMSIM** P-Code interpreter, from an Image File (**.IMG**);
- by the **ZCMDTERM** Terminal Program debugger, from a Debug File (**.DBG**).

2. The Terminal

The P-Code interpreter can run BasicCard programs simultaneously in the PC in simulated BasicCards, or it can communicate with genuine BasicCards via a card reader – a ZeitControl Chipi® or CyberMouse® card reader connected to a serial port or a USB port, or any other PC/SC-compatible card reader.

2.2.1 The Main Procedure

The *main procedure* starts at the first statement that is not contained inside a procedure definition, and ends at the start of the next procedure definition (or the end of the source file). The Terminal program begins execution at the first statement in the main procedure, and continues until it reaches the end of the main procedure, or until an **Exit** statement is executed.

2.2.2 Procedure Definitions

Procedure definitions in the Terminal program consist of functions and subroutines, exactly like a regular Basic program. Each procedure is self-contained – nested procedure definitions are not allowed, and **GoTo** and **GoSub** statements can only transfer control to labels within the current procedure.

2.2.3 Command Declarations

Before you can call a BasicCard command, you must declare it, so that the ZC-Basic compiler knows the two ID bytes of the command, and the types of the command parameters. Apart from the two ID bytes, a command declaration looks like a subroutine declaration. Here are declarations of the three example commands from **1.5 BasicCard Program Layout**:

```
Declare Command &H80 &H10 GetCustomerName (Name$)
Declare Command &H80 &H20 DebitAccount (Amount As Long)
Declare Command &H80 &H30 ChangeBalance (NewBalance As Long)
```

Calling these commands is just like calling a function:

```
Status = GetCustomerName (Name$)
If Status <> &H9000 And (Status And &HFF00) <> &H6100 Then
    Print "GetCustomerName: Status = &H"; Hex$ (Status)
    GoTo Retry
End If
```

You should always check the return value, even if the command itself has no error conditions, in case a communication problem has occurred (such as the card being removed from the reader). If you prefer, you can use the pre-defined variables **SW1**, **SW2**, and **SW1SW2**, which contain the status bytes from the most recently called command:

```
Call GetCustomerName (Name$)
If SW1SW2 <> &H9000 And SW1 <> &H61 Then
    Print "GetCustomerName: Status = &H"; Hex$ (SW1SW2)
    GoTo Retry
End If
```

See **7.6 Status Bytes SW1 and SW2** for a list of ZC-Basic status codes. The file `BasicCardPro\Inc\Commands.Def` defines these status codes in **Const** statements, so you can refer to &H9000 and &H61 as **swCommandOK** and **sw1LeWarning** respectively if you include this file in your program – see **3.3.1 Source File Inclusion**. Alternatively, you can call the subroutine **CheckSW1SW2()**, which is defined in the file `COMMERR.DEF`. If a communications error has occurred, this subroutine prints a suitable error message and exits.

2.2.4 Permanent Data

ZC-Basic contains a very convenient mechanism for the reading and writing of permanent data in the BasicCard: you just declare data of storage type **Eeprom**, and the BasicCard operating system does the rest. Although the Terminal program contains no genuine EEPROM data, this useful feature is available in Terminal programs as well, if they were loaded from a ZeitControl Image File (or Debug File). **Eeprom** data in a Terminal program is written back to the image file in two circumstances:

2.2 Terminal Program Layout

1. On program exit, if the appropriate options were specified:
 - in the **ZCMDTERM** Terminal Program debugger, checking the **Save Terminal EEPROM** entry in the **Terminal Program Options** dialog box;
 - with the **-W** parameter on the **ZCMSIM** command line (see **5.9.2 The P-Code Interpreter ZCMSIM.EXE**).
2. When the Terminal program executes a **Write Eeprom** statement (see **3.21.7 Saving Eeprom Data**).

Note: The **Write Eeprom** statement is only valid if the Terminal program is running in the **ZCMSIM** P-Code interpreter or the **ZCMDTERM** Terminal Program debugger. Programs containing **Write Eeprom** statements can't be compiled into executable files.

3. The ZC-Basic Language

The ZC-Basic programming language is a fully functional, modern Basic, with function and subroutine calls, user-defined data types, file I/O, and pre-processor directives. In addition, it has some special features for the smart card environment, including command definition and invocation, I/O encryption, and file access control.

In this chapter, the following conventions are observed:

- ZC-Basic keywords are printed in **bold text**.
- Statement fields that must be supplied by the programmer are printed in *italic text*.
- Programming examples are printed in **fixed-width bold text**.
- Optional statement fields are enclosed in [square brackets].
- Alternatives are separated by a vertical bar and enclosed in braces, e.g. { **ByVal** | **ByRef** }.

File I/O in ZC-Basic is described in **Chapter 4: Files and Directories**.

3.1 The Source File

A ZC-Basic program must consist of a single compilation unit – there is no linking stage. This lets the compiler work out the storage requirements of the whole program, so that it can use the limited RAM as efficiently as possible. You may, however, split your source into several files and **#Include** them all in a master source file.

The source consists of *lines*, which may be logically extended with the line continuation character ‘_’ (underscore). Each line consists of *statements*, separated from each other with ‘:’ (colon). A comment character ‘**’** (single quote) causes the rest of the line to be ignored (unless it occurs inside a string). The **Rem** keyword may also be used to introduce a comment, but it is only allowed at the beginning of a statement. For instance:

```
X = 0           '      Comment introduced by comment character
                Rem   OK to use Rem on its own line...
Y = 0 : Z = 0 : Rem ...but here we need the colon
```

3.2 Tokens

At the lowest level, a source program consists of a sequence of *tokens*. There are four kinds of token: constants, identifiers, reserved words, and special symbols. Except for string constants, tokens may not contain spaces or tabs.

A constant can be an integer, a floating-point number, or a string. Integer constants are decimal by default; the prefixes **&O** (or just **&**) and **&H** denote octal and hexadecimal constants respectively. Integer constants have the range –2147483648 to +2147483647.

If a constant contains a decimal point or an exponent (E or e), it is a floating-point constant. ZC-Basic supports only single-precision floating-point numbers. Floating-point numbers are stored in IEEE denormalised format, with an 8-bit exponent and a 23-bit mantissa. This gives a precision of 7 decimal places, and a range of 1.401298E–45 to 3.402823E+38.

A string constant is any sequence of printable characters enclosed in double quotes “”. To include non-printable characters in a string constant, use **Chr\$()**; the double quote itself is **Chr\$(34)**. For example:

```
X$ = Chr$(34) + "STRING" + Chr$(34) + Chr$(10) ' 10 = new line
```

Variables, procedures, etc. must be given names, or *identifiers*. In ZC-Basic, an identifier consists of letters (**A-Z**, **a-z**) and digits (**0-9**), followed by an optional type character (**@**, **%**, **&**, **!**, **\$**). It may be any length. An identifier must start with a letter. The type character specifies the data type of a function or variable, as follows:

Character:	@	%	&	!	\$
Data type:	Byte	Integer	Long	Single	String

If a type character is not present, the default type is **Integer** (but you can change this default behaviour with **DefByte**, **DefLng** etc – see 3.22.2 **DefType Statement**). Case is not significant in ZC-Basic, so **ABC**, **AbC**, and **abc** are considered identical. An identifier must not clash with a *reserved word*, which is a word with a pre-defined meaning.

Here is a list of the reserved words in ZC-Basic:

Abs	Access	And	Append	ApplicationID
As	Asc	At	ATR	Base
Binary	ByRef	Byte	ByVal	Call
CardInReader	CardReader	Case	Certificate	ChDir
ChDrive	Chr\$	Close	Cls	Command
Const	CurDir	CurDrive	Declare	DefByte
DefInt	DefLng	DefSng	DefString	DES
Dim	Dir	Disable	Do	Dynamic
Eeprom	Else	ElseIf	Enable	Encryption
End	EOF	Erase	Exit	Explicit
File	For	FreeFile	Function	Get
GetAttr	GoSub	GoTo	Hex\$	If
InKey\$	Input	Integer	Is	Key
Kill	LBound	LCase\$	Left\$	Len
Let	Line	Lock	Log	Long
Loop	LTrim\$	Mid\$	MkDir	Mod
Name	Next	Not	On	Open
Option	Or	Output	OverflowCheck	PcscCount
PcscReader	Peek	Poke	Polynomials	Print
Private	Public	Put	Random	Randomize
Read	ReDim	Rem	ResetCard	Return
Right\$	RmDir	Rnd	RTrim\$	Seek
Select	SetAttr	Shared	Single	Space\$
Spc	Sqrt	Static	Step	Str\$
String	String\$	Sub	Tab	Then
Time\$	To	Trim\$	Type	UBound
UCase\$	Unlock	Until	Val!	Val&
ValH	WEnd	While	Write	WTX
Xor				

In addition to constants, identifiers, and reserved words, the following special symbols are recognised:

_	Underscore (line continuation)	'	Single quote (comment character)
(Left parenthesis)	Right parenthesis
+	Plus	-	Minus
*	Multiply	/	Divide
,	Comma	:	Colon
=	Equals	<>	Not equals
<	Less than	>	Greater than
<=	Less than or equal to	>=	Greater than or equal to
.	Full stop or Period	#	Pre-processor directive or file number
;	Semi-colon	"	Double quote (string delimiter)

3. The ZC-Basic Language

3.3 Pre-Processor Directives

Pre-processor directives are instructions to the **ZCMBASIC** compiler. For instance, they tell the compiler which lines of source code to compile, and whether these lines should be written to the list file if a listing is requested. They can also be used to specify various command-line parameters in the source code itself – in this case, the compiler accepts the first occurrence of the parameter, so directives in the source code are overridden by parameters on the command line.

A pre-processor directive begins with the hash character ‘#’, which must be the first character on the input line (excluding spaces and tabs).

3.3.1 Source File Inclusion

The directive

#Include *filename*

causes the named file to be included and compiled as if it was part of the source file itself. Included files can themselves contain **#Include** directives, nested to any depth. If *filename* contains any space characters, it must be enclosed in double quotes (“*filename*”); otherwise the quotes are optional. The compiler looks for the file in the following directories:

- first, the directory of the including file;
- next, directories specified in **-I** parameters, in the order that they appear in the command line (see **5.9.1 The ZC-Basic Compiler ZCMBASIC.EXE**);
- next, the current directory;
- next, directories specified in the Windows Registry variable “**HKEY_CURRENT_USER\Software\ZeitControl\BasicCardPro\ZCINC**”;
- finally, directories specified in the **ZCINC** environment variable.

The **ZCINC** Windows Registry variable can be set from the **ZCPDE** Professional Development Environment, via menu item **Options|Environment|Compiler**.

3.3.2 Library Inclusion

The directive

#Library *filename*

loads a ZeitControl Plug-In Library for the Enhanced BasicCard. See **Chapter 6: Plug-In Libraries** for a list of currently available libraries. The compiler looks for the **#Library** file in the same directories as it looks for **#Include** files – see **3.3.1 Source File Inclusion** for details.

Notes:

- ZeitControl provides a definition file *library.def* for each library file *library.lib*. The definition file contains the appropriate **#Library** directive, along with all the required declarations. You should normally just **#Include** this definition file, rather than loading the library yourself with a **#Library** directive.
- Terminal programs and Professional BasicCard programs don’t need the **#Library** directive, as they use a different mechanism for loading Plug-In Libraries – see **3.13.2 Plug-In Library Procedures**.

3.3.3 Options

Professional BasicCards have options that can be selected using the **#Option** directive. At the time of writing, the following options are available in some or all cards:

Protocol Selection

#Option *protocol* [, *protocol*]

where *protocol* is either **T=0** or **T=1**. This enables one or both communication protocols. All Professional BasicCards support this option. Without this option, the enabled protocols depend on the card version – see **Professional BasicCard Datasheet** for details.

Inverse Convention

#Option InverseConvention

By default, all cards use the *Direct Convention* to encode the bytes exchanged with the Terminal: logic level ONE is high, and the least significant bit is sent first. Some cards also support the *Inverse Convention*, where logic level ONE is low, and the most significant bit is sent first. You won't need this option unless you are using old card readers that don't support the Direct Convention.

At the time of writing, this option is available in Professional BasicCards **ZC5.4** (from Revision B) and **ZC5.5** (all revisions).

SW1-SW2 = &H9XXX Allowed

#Option Allow9XXX

Normally, if *SW1-SW2* <> &H9000, and *SW1* <> &H61, then **ODATA** is not sent – see **7.5 Commands and Responses**. You can override this behaviour in some Professional BasicCards with this option: if *SW1-SW2* has the form &H9XXX, then **ODATA** is sent in the response. This behaviour is enabled for every command. See **6.8.8 SW1-SW2 Processing** for an alternative method.

At the time of writing, this option is available in Professional BasicCards **ZC5.4** (from Revision B) and **ZC5.5** (all revisions).

3.3.4 *Conditional Compilation*

Sections of code can be included or excluded according to the values of constants defined earlier (or on the compiler command line):

```
#If condition1
    code block 1
[ #ElseIf condition2
    code block 2 ]
[ #ElseIf condition3
    code block 3 ]
...
[ #Else
    code block n ]
#EndIf
```

where *condition1*, *condition2*,... are constant numerical expressions, which may include symbols defined in **Const** statements or on the compiler command line (with the “-Dsymbol” parameter – see **5.9.1 The ZC-Basic Compiler ZCMBASIC.EXE**). *Code block i* is compiled if *condition i* is the first non-zero condition.

Instead of testing the value of a numerical expression, you can test whether a constant symbol has been defined:

```
#IfDef symbol1
    code block 1
[ #ElseIfDef symbol2
    code block 2 ]
[ #ElseIfDef symbol3
    code block 3 ]
...
[ #Else
    code block n ]
#EndIf
```


3. The ZC-Basic Language

The directives **#IfNotDef** and **#ElseIfNotDef** have the opposite sense to directives **#IfDef** and **#ElseIfDef** respectively.

#EndIf has the alternative form **#End If** (with a space) for compatibility with the Basic **End If** statement.

See also **3.3.12 Pre-Defined Constants**.

3.3.5 Listing Directives

You can cause sections of code (or complete included files) to be omitted from the listing file with the directive

#NoList

The **#NoList** directive is cancelled by **#List**.

3.3.6 Card State

By default, the BasicCard is switched to state **TEST** after a ZC-Basic program is downloaded. You can override this with the **#State** directive:

#State { LOAD | PERS | TEST | RUN }

This is equivalent to the command-line parameter **-Sstate** (see **5.9.1 The ZC-Basic Compiler ZCMBASIC.EXE**).

3.3.7 Number of Open File Slots

Each open file in a ZC-Basic program is assigned an *open file slot*. The Terminal program has 32 open file slots, so the maximum number of files that can be opened simultaneously is fixed at 32. In the BasicCard, the default number of open file slots is 2, but this can be overridden with the **#Files** directive:

#Files *nFiles*

with $0 \leq nFiles \leq 16$. This number includes files opened in the BasicCard program and BasicCard files opened from a Terminal program. The amount of RAM used by the file system is $(6 * nFiles + 7)$ bytes (unless *nFiles* is zero, in which case no file system is installed, so no RAM is required).

3.3.8 Stack Size

The **#Stack** directive specifies the size of the P-Code stack:

#Stack *stack-size*

This is equivalent to the compiler command-line parameter **-Sstack-size** (see **5.9.1 The ZC-Basic Compiler ZCMBASIC.EXE**). If no stack size is specified, the compiler works out for itself how big the stack should be.

3.3.9 Message Directive

You can output a message at any point during compilation with

#Message *message*

The message is printed to the screen, and compilation continues unaffected.

3.3.10 Error Directive

You can define your own compiler error messages with the **#Error** directive. For instance:

```
#If MaxLineLength > 80
#Error MaxLineLength too big (max 80)
#EndIf
```

Then if anybody tries to compile the program with **MaxLineLength** defined as 100, say, the compiler will issue the error message **"#Error MaxLineLength too big (max 80)"** and stop compilation.

3.3.11 Block Waiting Time

In a BasicCard program that uses the **T=1** protocol, the **BWT** field in the **ATR** can be specified with

#BWT *n*

where *n* is a power of 2 between 1 and 512 inclusive. This Block Waiting Time specifies the time that the card is given to execute a command, before the card reader returns with status **swCardTimedOut**. It is expressed in tenths of a second (giving a maximum of 51.2 seconds). Its default value is 16 (1.6 seconds) in a Compact BasicCard, and 128 (12.8 seconds) in Enhanced and Professional BasicCards.

Cards that use the **T=0** protocol are restricted to a **WWT** (Work Waiting Time) of 128, i.e. 12.8 seconds.

3.3.12 Pre-Defined Constants

According to the target machine (Terminal, Compact BasicCard, Enhanced BasicCard, or Professional BasicCard), one of the following constants is pre-defined by the compiler (and has the value 1):

TerminalProgram CompactBasicCard EnhancedBasicCard ProfessionalBasicCard

For instance:

```
#IfNotDef EnhancedBasicCard
#Error This program must be compiled for the Enhanced BasicCard!
#EndIf
```

In BasicCard programs, the constants **CardMajorVersion** and **CardMinorVersion** are also defined. For instance, in a program compiled for the Enhanced BasicCard ZC3.5, they take the values 3 and 5 respectively.

3.4 Data Storage

All variables in a ZC-Basic program belong to one of four *data storage* classes: **Eeprom**, **Public**, **Static**, or **Private**.

3.4.1 Eeprom data

EEPROM is the BasicCard's equivalent of a hard disk. It retains its contents while the card is powered down in the customer's pocket. EEPROM contains your ZC-Basic program (compiled into P-Code), directories and files (in the Enhanced BasicCard), and all permanent variables (such as the customer's name or the credit balance in the card). For example:

```
Eeprom CustomerName$ = "" ' We don't know customer's name yet
Eeprom Balance& = 500     ' Free 5-euro bonus for new members
```

If you don't specify an initial value, the data will be initialised to zero. This initialisation takes place when the program (P-Code and data) is downloaded to the card.

Eeprom data has global scope – it can be accessed by all procedures in the program.

3.4.2 Public and Static data

The RAM data area contains **Public** and **Static** data, that retains its value as long as the BasicCard remains powered up in the card reader. **Public** data has global scope; **Static** data has local scope – it can only be accessed by the procedure that declared it.

Public and **Static** data can be initialised, just like **Eeprom** data. The initialisation takes place every time the card is powered up.

3.4.3 Private data

Data declared in a procedure as **Private** exists only until the procedure returns. It is allocated on the P-Code stack every time the procedure is called. It has local scope. **Private** data can be initialised with constant values:

3. The ZC-Basic Language

```
Private LoopCounter = 100
```

This initialisation takes place every time the procedure is called. Uninitialised **Private** data is set to zero when the procedure is called.

You don't have to declare every variable before you use it. If the compiler meets a variable name that it doesn't recognise, it implicitly declares it as **Private** – unless you have overridden this behaviour with the **Option Explicit** statement (see 3.22.4 **Explicit Declaration of Variables and Arrays**), or by declaring the procedure itself **Static** (see 3.12 **Procedure Definition**).

3.5 Data Types

ZC-Basic supports the following data types:

Byte	1-byte unsigned integer. Range: 0 to 255.
Integer	2-byte signed integer. Range: -32768 to +32767.
Long	4-byte signed integer. Range: -2147483648 to +2147483647.
Single	4-byte single-precision floating-point number (denormalised IEEE format: 1 sign bit, 8-bit exponent, and 23-bit mantissa with implied msb=1 unless exponent is zero). Precision: 7 decimal digits. Range: +/-1.401298E-45 to +/-3.402823E+38.
String	Character string, up to 254 bytes long. Requires $n+3$ bytes of storage, where n is the length of the string – a 2-byte pointer to an $(n+1)$ -byte (length, data) pair.
String*n	Fixed-length string, n bytes long, where n is a constant between 1 and 254. Requires n bytes of storage.

You may also define your own data types – see 3.8 **User-Defined Types**.

Note: The **Single** data type is not supported in the Compact BasicCard. You may store **Single** data in the Compact BasicCard, but you can't perform floating-point arithmetic operations or string conversions.

3.6 Arrays

An array in ZC-Basic can belong to any of the four data storage classes (**Eeprom**, **Public**, **Private**, **Static**), and its elements may be of any type (**Byte**, **Integer**, **Long**, **Single**, **String**, **String*n**, or a user-defined type). It may have up to 32 dimensions, and may contain up to 16K of data. In Compact and Enhanced BasicCard programs, the upper and lower bounds for each dimension are subject to the constraints:

$$-32 \leq \text{lower bound} \leq 31 \quad \text{and} \quad \text{lower bound} \leq \text{upper bound} \leq \text{lower bound} + 1023$$

All arrays are either **Dynamic** or **Fixed**. The upper and lower bounds of a **Fixed** array must be constant expressions, and can't be changed. The bounds of a **Dynamic** array can be any integer expression, and the array can be re-sized at any time with a **ReDim** statement. However, the number of dimensions of a **Dynamic** array can't be changed.

If any of the subscripts in an array access is out of bounds, a run-time P-Code error is generated.

The **ReDim** statement has the following syntax:

```
ReDim array (bounds [, bounds, ...]) [As type] [, array (bounds [, bounds, ...]) [As type], ...]
```

array If *array* has already been declared, it must be a **Dynamic** array, and one *bounds* specifier must be present for each dimension. (In this case, **As type** is not required, but if present it must match the type as originally declared.) If *array* has not yet been declared, then the **ReDim** statement does double duty as a data declaration statement. In other words, the statement

```
ReDim array (bounds [, bounds, ...]) [As type]
```

is expanded to

Dim *Dynamic* *array* ([, , . . .]) [**As** *type*]
ReDim *array* (*bounds* [, *bounds*, . . .])

(The **Dim** statement is described in 3.7 Data Declaration.)

bounds The *bounds* specifier gives the upper and lower bounds for each dimension, in the form [*lower-bound To upper-bound*]. If *lower-bound* is not given, it defaults to 0, unless otherwise specified in an **Option Base** statement (see 3.22.3 Array Subscript Base).

An array can be cleared with the **Erase** statement:

Erase *array* [, *array*, . . .]

If *array* is **Fixed**, all its elements are set to zero. If *array* is **Dynamic**, its data area is freed. In either case, if the elements of *array* are of type **String**, they are all freed.

3.7 Data Declaration

Data items and arrays are declared and initialised in a *data declaration statement*. A data declaration statement consists of a sequence of data declarations separated by commas. Data may optionally be initialised with constant values:

storage-class [**Dynamic**] *data-declaration* [=initial-value] [, *data-declaration* [=initial-value], . . .]

storage-class This can be **Eeprom**, **Public**, **Private**, or **Static**. The keyword **Dim** is also allowed; outside a procedure, **Dim** is a synonym for **Public**, and inside a procedure, it has the same meaning as **Private** (or **Static** in a procedure declared as **Static**).

Dynamic If the **Dynamic** keyword is present, then all arrays declared in the statement are **Dynamic** arrays.

data-declaration This field takes one of two forms:

1. For scalar (non-array) data, *data-declaration* has the form

name [**As** *type*] [**At** *address*]

The type of the variable *name* is determined as follows:

- by *type* if [**As** *type*] is present;
- otherwise, by the last character of *name* if it belongs to the following list:

Character:	@	%	&	!	\$
Data type:	Byte	Integer	Long	Single	String
- otherwise, by the initial character of *name*, as specified in the most recent **DefType** statement (see 3.22.2 DefType Statement).

By default, all initial characters are assigned to **Integer** type in ZC-Basic, as if by the statement **DefInt A–Z**.

The address of the variable *name* is automatically assigned by the compiler, unless overridden by [**At** *address*]. If present, *address* takes the form *var*[+*constant*], where *var* is the name of a previously declared variable. The new variable must be entirely contained within the previously-declared variable.

2. If an array is being declared, *data-declaration* has the form

array (*bounds* [, *bounds*, . . .]) [**As** *type*]

The type of the elements of the array is determined as described above for scalar variables. The form of the bounds specifier is described in the previous section under **ReDim**. There is an additional possibility – the empty array syntax:

array ([, . . .]) [**As** *type*]

3. The ZC-Basic Language

This declares a **Dynamic** array, while deferring the allocation of the array to a later time. The following example declares empty **Dynamic** arrays **A1**, **A2**, and **A3** with one, two, and three dimensions respectively:

```
Dim A1()  
Dim A2(,)  
Dim A3(,,)
```

Otherwise, *array* is **Dynamic** if (i) the **Dynamic** keyword was specified; or (ii) any of its bounds is non-constant.

If no initialisation data is present, the data item or array is initialised to zero (or empty strings in the case of **String** data). In ZC-Basic, any type of data may be initialised, with two exceptions: **Dynamic** arrays with non-constant initial bounds, and **Private Dynamic** arrays. Initialisation data must be constant. If an array is initialised, the data must be specified in the order of the array elements, with the leftmost subscript varying the fastest ('column-major' order). For instance, the following example initialises each element of a 2x2 **String** array to contain an ASCII description of itself:

```
Option Base 1 ' Set lower bound of arrays to 1  
Private X$(2,2) = "X$(1,1)", "X$(2,1)", "X$(1,2)", "X$(2,2)"
```

If the end of the initialisation data is reached before the array has been filled, the rest of the array is initialised to zero (or empty strings for a **String** array).

Fixed-length **String*n** data can be initialised in two ways: as a string, or as a list of bytes. These two ways can be combined, but the string must be the last data item in the list. For example:

```
Eeprom S1 As String*5 = "ABC" ' Padded with two NULL bytes  
Public S2 As String*3 = &H81, &H82, &H83  
  
Private S3 As String*7 = 3, 4, "XYZ"  
Rem This is equivalent to:  
Rem Private S3 As String*7 = 3, 4, 88, 89, 90, 0, 0
```

3.8 User-Defined Types

ZC-Basic supports the user definition of structured data types:

```
Type type-name  
member-name [As type] [, member-name [As type], ...]  
member-name [As type] [, member-name [As type], ...]  
...  
End Type
```

type-name and *member-name* are regular identifiers. The *type* of each member can be **Byte**, **Integer**, **Long**, **Single**, **String*n**, or another user-defined type. It may not be an array, or a **String** of variable length. The total size of all the members must not exceed 254 bytes.

If *var* is a variable or array element of type *type-name*, then the members of *var* are referred to using the syntax *var.member-name* (as in the 'C' programming language). For example:

```
Type Point: X!, Y!: End Type ' Character '!' => type Single...  
  
Type Rectangle  
Area As Single ' ...or the type can be declared explicitly  
TopLeft As Point  
BottomRight As Point  
End Type  
  
Sub Area (R As Rectangle)  
Width! = R.BottomRight.X! - R.TopLeft.X!  
Height! = R.BottomRight.Y! - R.TopLeft.Y!  
R.Area = Width! * Height!  
End Sub
```


A user-defined type can be copied as a unit, with a single assignment statement:

```
Public UnitSq As Rectangle = 0,0,0,1,1 ' BottomRight = (1.0,1.0)
Call Area (UnitSq) ' Fill in the Area
Public RA(10) As Rectangle
For I = 1 To 10 : RA(I) = UnitSq : Next I
```

Variables or array elements of the same user-defined type can be compared for equality using = and <> (but the comparison operators <, >, <=, and >= are not allowed).

3.9 Expressions

An *expression* is built up by applying *operations* to *terms*. For example:

```
X + 5          ' Apply '+' (addition) to terms X and 5
A(I) * Rnd     ' Apply '*' (multiplication) to terms A(I) and Rnd
S$ + "0"       ' Apply '+' (concatenation) to terms S$ and "0"
```

A term can be one of the following:

- A constant: the type of a constant term is **Byte**, **Integer**, or **Long** (depending on the value of the constant) for whole-number expressions, **Single** for floating-point expressions, and **String** for string constants.
- A scalar variable, an array element, or a member of a variable or array element of user-defined type.
- A function call. This can be a user-defined function or command, or a built-in function (such as **Abs**, **Sqrt**, **LBound**, **Chr\$**, or **CurDir**).
- An array name, with no parentheses (or an empty pair of parentheses). This returns the address of the data area of the array, so that you can check whether a dynamic array has been allocated or not. For instance:

```
Eeprom Dynamic A() ' Declare an Integer array
...
If A = 0 Then Redim A (10) ' or 'If A() = 0...'
```

An expression has one of the following types: **Byte**, **Integer**, **Long**, **Single**, **String**, *boolean*, or *user-defined*. A boolean expression is an expression of type **Integer** that is the result of a comparison; it takes the value **True** (–1) or **False** (0). Normally a boolean expression is treated the same as an **Integer** expression; any exceptions are noted below.

3.9.1 Numerical Expressions

If *expr1* and *expr2* are numerical expressions (i.e. expressions of type **Byte**, **Integer**, **Long**, **Single**, or *boolean*), the following operations are allowed, grouped in descending order of priority:

Group 1	– <i>expr1</i>	Unary minus
	+ <i>expr1</i>	Unary plus (has no effect)
Group 2	Not <i>expr1</i>	Bitwise complement
Group 3	<i>expr1</i> * <i>expr2</i>	Multiplication
	<i>expr1</i> / <i>expr2</i>	Division
	<i>expr1</i> Mod <i>expr2</i>	Remainder
Group 4	<i>expr1</i> + <i>expr2</i>	Addition
	<i>expr1</i> – <i>expr2</i>	Subtraction

3. The ZC-Basic Language

Group 5	$expr1 < expr2$	True if $expr1$ is less than $expr2$
	$expr1 <= expr2$	True if $expr1$ is less than or equal to $expr2$
	$expr1 > expr2$	True if $expr1$ is greater than $expr2$
	$expr1 >= expr2$	True if $expr1$ is greater than or equal to $expr2$
Group 6	$expr1 = expr2$	True if $expr1$ is equal to $expr2$
	$expr1 <> expr2$	True if $expr1$ is not equal to $expr2$
Group 7	$expr1 \text{ And } expr2$	Bitwise And
Group 8	$expr1 \text{ Xor } expr2$	Bitwise exclusive-or
Group 9	$expr1 \text{ Or } expr2$	Bitwise Or

The priority of an operator determines the order of the operations. For instance, $3 + -5 * 7$ is evaluated as $3 + ((-5) * 7)$, and $A \text{ Or } B \text{ And } C$ is evaluated as $A \text{ Or } (B \text{ And } C)$.

Groups 1, 3, and 4 are the *numerical operators*. The type of the resulting expression is determined as follows:

- If $expr1$ or $expr2$ is **Single**, then the other is converted to **Single** if necessary, and the resulting expression is of type **Single**.
- Otherwise, if $expr1$ or $expr2$ is **Long**, then the other is converted to **Long** if necessary, and the resulting expression is of type **Long**.
- Otherwise, $expr1$ and $expr2$ are converted to **Integer**, and the resulting expression is of type **Integer**.

Note: Even if $expr1$ and $expr2$ are both **Byte** expressions, they are converted to **Integer** before any operation is performed. (This means that the only expressions of type **Byte** are those consisting of a single term.)

Groups 5 and 6 are the *comparison operators*. Exactly the same conversions are applied as for the numerical operators, but the type of the resulting expression is boolean.

Groups 2, 6, 7, and 8 are the *bitwise operators*. Bitwise operations are never performed on **Single** expressions; if $expr1$ or $expr2$ is **Single**, it is converted to **Long** before a bitwise operation is performed. If both $expr1$ and $expr2$ are of boolean type, then the result is also of boolean type.

There is a special rule concerning the evaluation of expressions of boolean type:

If $expr1$ and $expr2$ are both of boolean type, and one of the expressions	
$expr1 \text{ And } expr2$	$expr1 \text{ Or } expr2$
occurs in the program, then $expr2$ is not evaluated if the value of the whole expression can be deduced from the value of $expr1$ alone.	

In other words:

- if $expr1$ is **False**, then “ $expr1 \text{ And } expr2$ ” is always **False** as well, so $expr2$ is not evaluated;
- if $expr1$ is **True**, then “ $expr1 \text{ Or } expr2$ ” is always **True** as well, so $expr2$ is not evaluated.

This is important if the evaluation of $expr2$ has any side-effects. For instance:

If X! = 0 Or F(1/X!) > 100 Then Goto 100

If $X!$ is zero, then $1 / X!$ is not evaluated (which would otherwise cause a run-time error), and the function **F** is not called (which might, for instance, have changed **Public** data).

3.9.2 String Expressions

If either *expr1* or *expr2* is of type **String**, then the other must be of type **String** as well: there are no mixed numerical/string operations. The following string operations are allowed:

Group 1	<i>expr1</i> + <i>expr2</i>	String concatenation
	<i>expr1</i> < <i>expr2</i>	True if <i>expr1</i> is less than <i>expr2</i>
Group 2	<i>expr1</i> <= <i>expr2</i>	True if <i>expr1</i> is less than or equal to <i>expr2</i>
	<i>expr1</i> > <i>expr2</i>	True if <i>expr1</i> is greater than <i>expr2</i>
	<i>expr1</i> >= <i>expr2</i>	True if <i>expr1</i> is greater than or equal to <i>expr2</i>
Group 3	<i>expr1</i> = <i>expr2</i>	True if <i>expr1</i> is equal to <i>expr2</i>
	<i>expr1</i> <> <i>expr2</i>	True if <i>expr1</i> is not equal to <i>expr2</i>

The resulting expression is of **String** type after string concatenation (Group 1), and of boolean type after string comparison (Groups 2 and 3). The comparison operations in Group 2 are performed by finding the first characters that differ in the two strings, and comparing their ASCII values. In ASCII, all lower-case letters are greater than all upper-case letters, so for instance “abc” is greater than “XYZ”. For case-insensitive comparison, use **UCase\$** or **LCase\$** to convert both arguments to the same case. For example:

If UCase\$(S1\$) > UCase\$(S2\$) Then T\$ = S1\$: S1\$ = S2\$: S2\$ = T\$

3.9.3 Expressions of User-Defined Type

The only operation allowed on user-defined types is comparison for equality:

Group 1	<i>expr1</i> = <i>expr2</i>	True if <i>expr1</i> is equal to <i>expr2</i>
	<i>expr1</i> <> <i>expr2</i>	True if <i>expr1</i> is not equal to <i>expr2</i>

The resulting expression is of boolean type.

3.10 Assignment Statements

An assignment statement has the form

[Let] *var* = *expression*

where *var* is a scalar variable, or an array element, or a member of a variable or array element of user-defined type. The **Let** keyword is optional. The following rules apply:

- If *var* has numerical type (**Byte**, **Integer**, **Long**, or **Single**), then *expression* must have numerical type.
- If *var* has type **String** or **String*n**, then *expression* must have type **String**.
- If *var* has a user-defined type, then *expression* must have the same user-defined type.

There are four special string assignment statements:

[Let] Mid\$ (*string*, *start* [, *length*]) = *expression*

[Let] Left\$ (*string*, *length*) = *expression*

[Let] Right\$ (*string*, *length*) = *expression*

[Let] *string* (*n*) = *expression*

Mid\$ overwrites *length* characters of *string* with the value *expression*, starting from position *start*. (The first character in the string has position 1.) A value of *start* less than 1 results in a run-time error; a value of *start* greater than the length of *string* is not an error, but no characters are copied. If *length* is

3. The ZC-Basic Language

absent, or if *start+length* is greater than the length of *string*, the whole of rest of the string is overwritten.

Left\$ overwrites the first *length* characters of *string* with the value *expression*. If *length* is greater than the length of *string*, the whole of *string* is overwritten.

Right\$ overwrites the last *length* characters of *string* with the value *expression*. If *length* is greater than the length of *string*, the whole of *string* is overwritten.

In ZC-Basic, *string* (*n*) is shorthand for **Mid\$** (*string*, *n*, 1). So the last statement in the above list assigns the first character of *expression* to the *n*th character of *string*.

In the first three string assignment statements, only the first *length* characters of *expression* are copied into *string*. If *length* is greater than the length of *expression*, then the destination sub-string is filled out with NULL characters (i.e. ASCII zeroes).

3.11 Program Control

3.11.1 Exit Statements

An **Exit** statement jumps out of an enclosing block of code, according to the type of the statement:

Exit For	Jumps to the statement following the innermost current For -loop.
Exit While	Jumps to the statement following the innermost current While -loop.
Exit Do	Jumps to the statement following the innermost current Do -loop.
Exit Case	Jumps to the statement following the next End Select .
Exit Sub	Returns from a subroutine to the calling procedure.
Exit Function	Returns from a function to the calling procedure.
Exit Command	Returns from a BasicCard command to the caller in the Terminal program.
Exit	Exits the program. Exit in a Terminal program returns to the operating system; Exit in a BasicCard program returns to the caller in the Terminal program. <i>Note:</i> The Exit statement (with no parameters) exits the program immediately, without freeing Private strings and arrays. This is not a problem in the Terminal program, but it can cause pcOutOfMemory errors in subsequent commands in a BasicCard program, until the card is reset. So you should only use such an Exit statement in a BasicCard program if you detect an error condition that prevents the card from continuing the command-response session.

3.11.2 Labels

There are two types of label in ZC-Basic: named labels, and line numbers. A named label is an identifier followed by a colon. A line number is simply a decimal number, which may or may not be followed by a colon. A label, of either type, may only be accessed from within the procedure that defines it. Label names and line numbers must be unique within each procedure, but the same name or line number can be used in two different procedures.

3.11.3 GoTo

The simplest program control statement is the **GoTo** statement:

```
GoTo label  
...  
label:
```

The program continues execution at the statement following *label*.

Note: You can't use **GoTo** to jump from one procedure to another.

3.11.4 GoSub

A procedure can call its own private subroutines with the **GoSub** statement. Such a private subroutine is not a procedure; it has no parameters, and no data of its own. It is simply a part of the procedure that defines it. It returns with the **Return** statement:


```

GoSub label
...
label:
    subroutine-code
Return [return-label]

```

If *return-label* is specified in the **Return** statement, the subroutine returns there; otherwise it returns to the statement following the **GoSub** call.

3.11.5 If-Then-Else

The **If** statement executes code depending on the value of a conditional expression:

```

If condition Then
    code block
End If

```

The full form of the **If-Then-Else** block is as follows:

```

If condition1 Then
    code block 1
[ElseIf condition2 Then
    code block 2
[ElseIf condition3 Then
    code block 3
...
[Else
    code block n
End If

```

Each condition is a numerical expression. *code block i* is executed if *condition i* is non-zero (true). If all the conditions are zero (false), then *code block n* is executed.

If there are any statements on the same line after the **Then** of the initial **If**-statement, then this is a *single-line If-statement*. In this case, the **If-Then-Else** block is terminated not with **End If**, but with the end of the line. (This is the only place in the ZC-Basic language where a colon is not equivalent to an end of line.) For instance:

```

If X = 0 Then GoTo 100
If X < 0 Then X = 0 : ElseIf X > 50 Then X = 50

```

This is equivalent to

```

If X = 0 Then
    GoTo 100
End If

If X < 0 Then
    X = 0
ElseIf X > 50 Then
    X = 50
End If

```

3.11.6 For-Loop

The **For**-loop executes a block of code a specified number of times:

```

For loop-var = start To end [Step increment]
    [code block]
[Exit For]
    [code block]
Next [loop-var]

```

loop-var A numerical variable, used to count the number of times the **For**-loop has been executed.

3. The ZC-Basic Language

<i>start</i>	A numerical expression, the initial value of <i>loop-var</i> .
<i>end</i>	A numerical expression. The For -loop terminates when <i>loop-var</i> passes this value. More precisely: If <i>increment</i> ≥ 0 , then the For -loop terminates when <i>loop-var</i> $> end$. If <i>increment</i> < 0 , then the For -loop terminates when <i>loop-var</i> $< end$.
<i>increment</i>	The amount by which <i>loop-var</i> is incremented after each execution of the For -loop. If [Step <i>increment</i>] is absent, <i>increment</i> takes the value 1.

The **Exit For** statement breaks out of the **For**-loop to the statement following the **Next** instruction.

loop-var is optional in the **Next** statement (but it can be useful as a reminder if the loop is large).

If **For**-loops are nested, the **Next** statement can specify more than one loop variable. For example:

```
For I = 1 To 10: For J = 1 To 10: A(I,J) = 0 : Next I, J
```

Note: The **Exit For** statement breaks out of only the innermost **For**-loop, even if the **Next** statement specifies more than one loop variable. So the following example prints the values **11** and **21**:

```
For I = 1 To 2 : For J = 1 To 2  
Print 10*I + J : Exit For  
Next I, J
```

3.11.7 While-Loop and Do-Loop

The **While**-loop is executed as long as *condition* is non-zero:

```
While condition  
    [code block]  
    [Exit While]  
    [code block]  
Wend
```

The **Do**-loop has more flexibility:

```
Do [{While | Until} condition]  
    [code block]  
    [Exit Do]  
    [code block]  
Loop [{While | Until} condition]
```

The optional [{**While** | **Until**} *condition*] may appear at the beginning or the end of the **Do**-loop, but not both. If it appears at the end, then the loop is always executed at least once. If neither is present, then the loop is executed endlessly until left by some other means (such as **Exit Do** or **GoTo**).

3.11.8 Select Case

The **Select Case** statement executes one of several blocks of code, depending on the value of a test expression:

```
Select Case test-expression  
Case case-test [, case-test, ...]  
    [code block]  
    [Exit Case]  
    [code block]  
Case case-test [, case-test, ...]  
    [code block]  
    [Exit Case]  
    [code block]  
...  
[Case Else  
    [code block]  
    [Exit Case]  
    [code block ]  
End Select
```


test-expression An expression of any type (numerical, **String**, or user-defined)

case-test This takes one of three forms:

expression **True** if *test-expression* = *expression*

expr1 To expr2 **True** if *expr1* <= *test-expression* <= *expr2*

[**Is**] *op expr* **True** if *test-expression op expr*, where *op* is one of the six comparison operators: < <= > >= = <>

The **Is** keyword is optional.

If *test-expression* is of user-defined type, only the first of these three forms is valid.

The **Select Case** statement executes the code following the first **Case** statement that contains a *case-test* that is **True**. If more than one such **Case** statement exists, only the first is executed. If no such **Case** statement exists, then the code following the **Case Else** statement is executed (and if there is no **Case Else** statement, none of the code in the **Select Case** block is executed). The **Exit Case** statement jumps to the statement following **End Select**.

3.11.9 Computed GoTo and Computed GoSub

You can jump to one of a list of labels depending on the value of a test expression:

On *expression* { **GoTo** | **GoSub** } *label1* [, *label2*, . . . , *labeln*]

expression An expression of type **Integer**. If it is equal to *r*, with $1 \leq r \leq n$, then **GoTo** *labelr* or **GoSub** *labelr* is executed. If *expression* < 1 or *expression* > *n*, execution proceeds with the following statement.

3.12 Procedure Definition

A ZC-Basic program consists mainly of procedure definitions. Each procedure is either a **Subroutine**, a **Function**, or a **Command**. The **Private** and **Static** variables declared in a procedure belong to that procedure alone, and can't be accessed from other procedures (such variables are said to have local scope); **Public** and **Eeprom** variables can be accessed from all procedures (they have global scope).

3.12.1 Subroutine

The simplest procedure type is the subroutine. A subroutine returns no value to the caller, except through its arguments. A subroutine definition is as follows:

[**Static**] **Sub** *proc-name* ([*param-def*, *param-def*, . . .])
 [*procedure code*]
 [**Exit Sub**]
 [*procedure code*]

End Sub

Static If the **Static** keyword is present in the definition, undeclared variables in the procedure have **Static** storage class, instead of **Private**.

param-def [(**ByVal** | **ByRef**)] *param-name*[0] [**As type**], where *param-name* is a variable name by which the parameter is accessed in *procedure-code*. See **3.15 Procedure Parameters** for a full discussion of parameters.

3.12.2 Function

A **Function** is a **Subroutine** that returns a value to the caller. A function definition is as follows:

[**Static**] **Function** *proc-name* ([*param-def*, *param-def*, . . .]) [**As type**]
 [*procedure code*]
 [*proc-name* = *expression*]
 [**Exit Function**]
 [*procedure code*]

End Function

3. The ZC-Basic Language

Static If the **Static** keyword is present in the definition, undeclared variables in the procedure have **Static** storage class, instead of **Private**.

param-def [{**ByVal** | **ByRef**}] *param-name*[(0)] [**As type**], where *param-name* is a variable name by which the parameter is accessed in *procedure-code*. See **3.15 Procedure Parameters** for a full discussion of parameters.

The return type of the function is determined as if *proc-name* were a variable name: from [**As type**] if present; otherwise from the last character in *proc-name* if it is a type character (@, %, &, !, or \$); otherwise from the first character in *proc-name*. (The type characters are defined in **3.2 Tokens**.) A function can have any return type that is not an array.

Inside the function, *proc-name* behaves like a **Private** variable. It is initialised to zero when the function is called, and its value is returned to the caller when the function exits.

3.12.3 Command

A command is defined like a subroutine, but you must specify the two ID bytes (**CLA** and **INS**) by which the command will be invoked:

[**Static**] **Command** [**CLA**] [**INS**] *proc-name* ([*PreSpec*,] [*param-def*, *param-def*, . . .] [, *PostSpec*])
 [procedure code]
 [**Exit Command**]
 [procdedure code]

End Command

Static If the **Static** keyword is present in the definition, undeclared variables in the procedure have **Static** storage class, instead of **Private**.

CLA The ‘Class’ byte. All the pre-defined commands in the BasicCard have **CLA=&HC0**, so you should avoid this value for your own commands, unless you specifically want to override a pre-defined command. If **CLA** is not present, **CLA** must be present in *PreSpec*.

INS The ‘Instruction’ byte. The compiler accepts any value; but in a card that uses the **T=0** protocol, this byte must be even, and the top nibble may not be **6** or **9**. If **INS** is not present, **INS** must be present in *PreSpec*.

PreSpec Pre-parameter specification. It may contain the following terms, in the following order, and separated by commas:

CLA=constant	An alternative way of specifying CLA
INS=constant	An alternative way of specifying INS
Lc=0	Only relevant under the T=0 protocol

In a Professional BasicCard using the **T=0** protocol, **Lc=0** defines the command as having no incoming data – a **Case 2** command in the terminology of **7.3.2 APDU Transmission by T=0**. You only need to use this if:

- you are implementing a pre-existing **T=0** command specification; or
- you want to minimise **T=0** communications overhead to improve performance.

param-def [{**ByVal** | **ByRef**}] *param-name*[(0)] [**As type**], where *param-name* is a variable name by which the parameter is accessed in *procedure-code*. See **3.15 Procedure Parameters** for a full discussion of parameters.

PostSpec Post-parameter specification, only relevant under the **T=0** protocol. You only need to use this if:

- you are implementing a pre-existing **T=0** command specification; or
- you want to minimise **T=0** communications overhead to improve performance.

It may take one of two forms:

Disable Le
Input Le

Disable Le defines the command as having no outgoing data – a **Case 3** command in the terminology of **7.3.2 APDU Transmission by T=0**.

Input Le is used to distinguish the two sub-cases of **Case 4** commands – *Case 4S.2* and *Case 4S.3* in **7.3.6 Case 4: Incoming and Outgoing Data**. In *Case 4S.2* commands, **ResponseLength** is specified by the Terminal program in the **Le** parameter, so the Terminal program must send **Le** before the command is executed; in *Case 4S.3* commands, the BasicCard decides for itself what **ResponseLength** should be. **Input Le** defines the command as a *Case 4S.2* command.

Notes:

1. The special syntax “[**Static**] **Command Else** *proc-name* ([*param-def*, *param-def*, ...])” defines a *default command* in the card, that is called when the BasicCard receives a command with unrecognised *CLA* and *INS*.
2. A **Command** parameter may not be an array.
3. A **Command** definition is only valid in a BasicCard program; it is not allowed in a Terminal program.
4. If a **Command** parameter is a variable-length string, it must be the last (or only) parameter in the list. In the Compact BasicCard, the compiler must know how long this string can be, so that it can make sure the P-Code stack is large enough; you can specify a maximum length for the string with the special syntax:

param-name <= *maxlen*

For example:

```
Command &H20 &H00 SetUserName(UserID, Name$<=25)
```

In the absence of this special syntax, *maxlen* defaults to 40. (The Enhanced and Professional BasicCards use a more flexible mechanism, and the length of the string is limited only by the requirement that the total parameter list be no larger than 255 bytes. So this special syntax is not required.)

3.13 Procedure Declaration

The compiler can't process a procedure call unless it knows what kinds of parameters the procedure accepts. It knows this if the procedure has already been defined:

```
Function Square (X!) As Single
    Square = X! * X!
End Function

Sub S()
    Y! = Square (5.5)      ' OK - Square already defined
End Sub
```

But the compiler won't accept the following:

```
Sub S()
    Y! = Square (5.5)      ' Error - Square not defined yet
End Sub

Function Square (X!) As Single
    Square = X! * X!
End Function
```

To call a procedure before it is defined, you must provide a *procedure declaration* that tells the compiler what it needs to know. A procedure declaration starts with the word **Declare**:

```
Declare Sub proc-name ([param-def, param-def, ...])
Declare Function proc-name ([param-def, param-def, ...]) [As type]
Declare Command [CLA] [INS] proc-name ([PreSpec,] [param-def, param-def, ...] [, PostSpec])
```

If a declaration and a definition of the same procedure occur in the program, then they must match. More precisely:

3. The ZC-Basic Language

- for a **Function**, the return type in the declaration must match the return type in the definition;
- for a **Command**, *CLA* and *INS* must be the same in the declaration and the definition;
- the types of the parameters must match exactly;
- the parameter-passing method (**ByVal** or **ByRef**) must be the same for each parameter.

However, the names of the parameters don't need to match. Parameter names in a procedure declaration are just place-holders; the only restriction is that they may not be reserved words (see 3.2 **Tokens** for a list of reserved words). For example:

```

Declare Function Square (Z!) As Single
Sub S()
Y! = Square (5.5)           ' OK - Square declared
End Sub
Function Square (X!) As Single ' OK - matches declaration
Square = X! * X!
End Function

```

3.13.1 Command Declarations

A **Command** declaration has the following general form:

Declare Command [*CLA*] [*INS*] *proc-name* ([*PreSpec*,] [*param-def*, *param-def*, ...] [, *PostSpec*])

The *param-def* fields are the same as in **Function** and **Sub** declarations. The *PreSpec* and *PostSpec* fields are available for users who need precise control over the **T=0** and **T=1** Command APDU parameters; otherwise they are not required.

CLA The 'Class' byte. All pre-defined commands in the BasicCard have **CLA=&HC0**, so you should normally avoid this value for your own commands, unless you want to override a pre-defined command. If *CLA* is not present, **CLA** must be present in *PreSpec*, either here or in the procedure call – see 3.14.3 **Calling a Command**.

INS The 'Instruction' byte. The compiler accepts any value; but in a card that uses the **T=0** protocol, this byte must be even, and the top nibble may not be **6** or **9**. If *INS* is not present, **INS** must be present in *PreSpec*, either here or in the procedure call – see 3.14.3 **Calling a Command**.

PreSpec Pre-parameter specification. This field may contain any of the following terms, in the following order, and separated by commas:

```

CLA=constant
INS=constant
P1=constant
P2=constant
P1P2=constant
Lc=constant

```

Each *constant* is a **Byte** expression, except **P1P2**, which is an **Integer**. See 7.5 **Commands and Responses** for definitions of these terms.

PostSpec Post-parameter specification. If present, this field takes one of the following forms:

```

Le=constant
Disable Le

```

Here, *constant* is a **Byte** expression; **Disable Le** specifies that **Le** is absent from the command. See 7.5 **Commands and Responses** for a definition of **Le**.

3.13.2 Plug-In Library Procedures

In Terminal programs and Professional BasicCard programs, Plug-In Library procedures are called via the **SYSTEM** instruction. They are declared as follows:

Declare Sub *SysCode SysSubcode proc-name* ([*param-def*, *param-def*, ...])

Declare Function *SysCode SysSubcode proc-name* ([*param-def*, *param-def*, ...]) [**As type**]

SysCode The Plug-In Library identifier, a **Byte** between **&HC0** and **&HFF**.

SysSubcode The procedure sub-code, any **Byte** value.

3.14 Procedure Calls

3.14.1 Calling a Subroutine

The recommended way to call a subroutine is

Call *procedure-name* ([[**ByVal** | **ByRef**] *expression*, [**ByVal** | **ByRef**] *expression*, . . .])

The expressions in the list must match the parameters in the subroutine declaration (or definition) in number and type. (See **3.15 Procedure Parameters** below for a fuller explanation.) If the subroutine takes no parameters, then the parentheses are optional:

Call *procedure-name* [()]

Alternatively, ZC-Basic accepts the older subroutine call syntax (with parentheses not allowed):

procedure-name [[**ByVal** | **ByRef**] *expression*, [**ByVal** | **ByRef**] *expression*, . . .]

3.14.2 Calling a Function

A **Function** call returns a value, that can be used as a term in an expression. For example:

X! = X! + Square (X!+1)

A **Function** can also be called just as if it were a **Subroutine**, in which case the return value is simply discarded.

3.14.3 Calling a Command

A **Command** is called as if it were a **Function** – although it is defined as if it were a **Subroutine**. The reason for this is that the Terminal program automatically returns the command status word (**SW1–SW2**) as if it were the return value of a function. This command status word should always be checked, as it is possible that communications were disrupted for some reason before the command could be successfully completed in the BasicCard.

A **Command** call has the following general form:

var = *command-name* ([*PreSpec*,] *arg-list* [, *PostSpec*])

where the *arg-list* field is the same as in **Function** and **Sub** calls. The *PreSpec* and *PostSpec* fields are available for users who need precise control over the **T=0** and **T=1** Command APDU parameters; otherwise they are not required.

PreSpec Pre-parameter specification. This field may contain any of the following terms, in the following order, and separated by commas:

CLA=*expr*
INS=*expr*
P1=*expr*
P2=*expr*
P1P2=*expr*
Lc=*expr*

Each *expr* is a **Byte** expression, except **P1P2**, which is an **Integer**. See **7.5 Commands and Responses** for definitions of these terms.

PostSpec Post-parameter specification. If present, this field takes one of the following forms:

Le=*expr*
Disable Le

Here, *expr* is a **Byte** expression; **Disable Le** specifies that **Le** is absent from the command. See **7.5 Commands and Responses** for a definition of **Le**.

An alternative method of calling a command:

Call *command-name* ([*PreSpec*,] *arg-list* [, *PostSpec*])

In this case, the command status word is available in the pre-defined variables **SW1**, **SW2**, and **SW1SW2**.

3.15 Procedure Parameters

3.15.1 Parameter Passing

In traditional Basic, procedure parameters are passed *by value* or *by reference*. Passing by value means that the procedure receives its own copy of the parameter; any changes it makes to this copy are lost when the procedure returns. Passing by reference means that the address (or ‘reference’) of the parameter is passed to the procedure; knowing its address, the called procedure can change the value of a variable in the calling procedure.

In general, ZC-Basic can’t do this, because the BasicCard can’t change the value of a variable in the Terminal program directly. However, it uses a *write-back* mechanism to achieve the same effect (and it retains the keywords **ByVal** and **ByRef**, although they are not strictly accurate). With the exception of **String** and array parameters, all parameters are passed by value (in the traditional sense); the value of each parameter is pushed onto the P-Code stack before the procedure is called. The parameters are then referenced like **Private** variables in the called procedure, and can be read or written directly. Then when the procedure returns to the caller, any parameters that were passed **ByRef** are copied back from the stack into their original locations.

By default, all parameters are passed **ByRef** (in the ZC-Basic sense). If the **ByVal** keyword is specified in the procedure definition or declaration, then the following parameter is passed by value, and not written back when the procedure returns. (The **ByRef** keyword is also allowed here, although it is superfluous.) The parameter-passing method specified in the procedure definition or declaration can be overridden for a particular procedure call by specifying **ByVal** or **ByRef** in front of a parameter. (Here **ByRef** is not superfluous if the parameter was specified as **ByVal** in the procedure definition or declaration.)

For the write-back mechanism to be invoked for a given parameter, the parameter-passing method must be **ByRef**, and the expression in the procedure call must be an *assignable* expression – an expression that can appear on the left-hand side of an assignment statement. If you don’t want a variable to be changed by a called procedure, you can specify **ByVal**, or you can enclose the variable in parentheses (which is a valid expression, but not an assignable expression). An example may make this clearer:

```
Declare Sub S (X, ByVal Y, ByRef Z) ' 'ByRef' redundant here
Private A, B, C
Call S (A, B, C)                  ' A and C can change
Call S (ByVal A, ByRef B, C)      ' B and C can change
Call S (A+1, B, (C))              ' Nothing can change - 'A+1' and '(C)'
                                  ' are not assignable expressions
```

For information on the maximum total size of a parameter list, see **3.23.1 Parameter Size Limits**.

3.15.2 String Parameters

There is an important difference between parameters of type **String** and parameters of type **String*n**. The former occupy 3 bytes on the P-Code stack, the latter occupy *n* bytes. So you should where possible use **String** parameters rather than **String*n** parameters. However, a variable-length string parameter to a **Command** is only allowed if it is the last (or only) parameter; any other string parameters must be of fixed-length **String*n** type.

Note: You can pass a fixed-length string in a **String** parameter, or a variable-length string in a **String*n** parameter; the compiler performs the necessary conversions. The parameter type only determines how the string is passed to the procedure.

For more information on **String** parameters, see **3.23.3 String Parameter Format**.

3.15.3 Array Parameters

An array parameter takes up just two bytes on the P-Code stack (the address of the array descriptor is passed to the procedure – see **3.23.2 Array Descriptor Format**).

An array parameter is specified in a procedure definition or declaration by a pair of parentheses after the parameter name:

param-name() [**As type**]

The parentheses must be empty. To pass an array parameter in a procedure call, the array name is sufficient; an empty pair of parentheses after the array name is optional. The type of the array must match exactly the type of the parameter. For example:

```
Declare Sub S (A() As Integer) ' Parentheses required here
Dim X (10) As Integer, Y (20) As Long
Call S (X) ' OK
Call S (X()) ' Also OK - parentheses optional in call
Call S (Y) ' Error - Y is Long array, not Integer array
```

The number of dimensions of the array is checked at run-time. The following code will compile, but will generate a run-time error:

```
Declare Sub S (A() As Integer)
Dim X (5, 5, 5)
Call S (X)
...
Sub S (A() As Integer)
A (2, 2) = 0 ' Run-time error - parameter X has 3 dimensions
```

3.15.4 Parameters of User-Defined Type

A parameter of user-defined type is passed to a procedure by pushing every member onto the P-Code stack. The P-Code stack occupies precious RAM, so you should avoid passing large user-defined types as procedure parameters. Otherwise, a parameter of user-defined type behaves just like a parameter of numerical type.

3.16 Built-in Functions

3.16.1 Numerical Functions

- Abs(X)** Returns the absolute value of *X* (that is to say, *X* or $-X$, whichever is positive). The type of the result is the type of *X*, unless *X* is **Byte**, in which case **Abs(X)** has type **Integer**.
- Rnd** Returns a random number of type **Long**: $-2147483648 \leq \text{Rnd} \leq 2147483647$. See **3.18 Random Number Generation**.
- Sqrt(X)** Returns the square root of *X*. The result is of type **Single**.

3.16.2 Array Functions

- LBound(array [, dim])** These two functions return the lower and upper bounds of subscript *dim* in the given array. If *dim* is not present, the lower or upper bound for the first subscript is returned. The result is of type **Integer**.
- UBound(array [, dim])**

3.16.3 String Functions

- string (n)** Returns a string of length 1, containing the *n*th character of *string*. (The first byte of the string has position 1.) It is shorthand for **Mid\$(string, n, 1)**.
- Asc(string)** Returns the ASCII value of the first character of *string*, as a **Byte**.
- Chr\$(char-code)** Returns a string of length 1, containing the ASCII character with the given *char-code*.
- Hex\$(val)** Returns a string containing the hexadecimal representation of the **Long** number *val*.
- Left\$(string, len)** Returns the first *len* bytes of *string*.
- LCase\$(string)** Returns *string* with all upper-case letters converted to lower-case.
- Len(string)** Returns the length of *string*, as a **Byte**.

3. The ZC-Basic Language

LTrim\$(string)	Returns <i>string</i> with leading spaces and NULL bytes removed.
Mid\$(string, start[, len])	Returns <i>len</i> bytes of <i>string</i> , starting from position <i>start</i> . (The first byte of the string has position 1.) If <i>start</i> > Len(string) , the empty string is returned. If <i>start</i> + <i>len</i> > Len(string) , or if <i>len</i> is absent, then the whole of <i>string</i> from position <i>start</i> is returned. If <i>start</i> <= 0 or <i>len</i> < 0, a run-time error is generated.
Right\$(string, len)	Returns the last <i>len</i> bytes of <i>string</i> .
RTrim\$(string)	Returns <i>string</i> with trailing spaces and NULL bytes removed.
Space\$(len)	Returns a string containing <i>len</i> space characters (ASCII 32).
Str\$(val)	Returns a string containing the decimal representation of <i>val</i> . If <i>val</i> is of type Single , its value is given to 7 significant figures. <i>Note:</i> If <i>val</i> is of type Single , use of this statement in an Enhanced BasicCard program will reduce the amount of user-programmable EEPROM available – see 3.23.5 Single-to-String Conversion for details.
String\$(len, char)	Returns a string consisting of <i>len</i> characters with ASCII value <i>char</i> . If <i>char</i> is itself a string, then the returned string consists of <i>len</i> copies of the first character of <i>char</i> .
Trim\$(string)	Returns <i>string</i> with leading and trailing spaces and NULL bytes removed.
UCase\$(string)	Returns <i>string</i> with all lower-case letters converted to upper-case.
Val&(string[, len])	Returns the decimal number represented by <i>string</i> , as a Long value. If <i>len</i> is present, it must be a variable (not an array element). This variable is set to the number of characters used.
Val!(string[, len])	Returns the decimal number represented by <i>string</i> , as a Single value. If <i>len</i> is present, it must be a variable (not an array element). This variable is set to the number of characters used. <i>Note:</i> Use of this statement in an Enhanced BasicCard program will reduce the amount of user-programmable EEPROM available – see 3.23.5 Single-to-String Conversion for details.
ValH(string[, len])	Returns the hexadecimal number represented by <i>string</i> , as a Long value. If <i>len</i> is present, it must be a variable (not an array element). This variable is set to the number of characters used.

3.16.4 Encryption Functions

Note: These functions are not available in the Compact BasicCard.

Key(keynum)	Returns key number <i>keynum</i> as a string. If no such key exists, a zero-length string is returned. This function may also appear on the left of an assignment statement: Key(keynum) = string In the Terminal program, Key is a pre-defined, Static array of strings: Key(0 To 255) As String . In the Enhanced and Professional BasicCards, only keys declared in Declare Key statements can be accessed, and the length of each key is fixed; see 3.17.2 Key Declaration for details.
DES(type, key, block\$)	Performs a single DES block encryption or decryption operation, returning the result as an 8-byte string. <i>key</i> is either a key number from 0 to 255, or a string containing a cryptographic key. <i>block\$</i> is a string at least 8 bytes long. See 3.17.6 DES Encryption Primitives for more information. Professional BasicCards that support the AES Plug-In Library may not support this function.
Certificate(key, data)	Returns a cryptographic certificate of <i>data</i> , as an 8-byte string. <i>key</i> is either a key number from 0 to 255, or a string containing a cryptographic key. See 3.17.7 Certificate Generation for more information.

3.16.5 Other Functions

Len(variable)	Returns the size, in bytes, of a scalar variable (arrays are not allowed).
Len(type)	Returns the size of a data type (e.g. Integer , or a user-defined type).

3.17 Encryption

3.17.1 Implementing Encryption

The Compact, Enhanced, and Professional BasicCards contain a sophisticated mechanism for the encryption and decryption of commands and responses. For full details of the algorithms, see **Chapter 8: Encryption Algorithms**. To implement this mechanism for your commands:

1. Use the **KEYGEN** program to generate a key file, containing cryptographic keys (and primitive polynomials for the **SG-LFSR** algorithm if you are programming for the Compact BasicCard).
2. Include the generated key file in both the Terminal program and the BasicCard program.
3. Include the file **COMMANDS.DEF** in the Terminal program, to define the **StartEncryption**, **ProEncryption**, and **EndEncryption** commands.
4. In the Terminal program, turn automatic encryption on and off as follows:

Compact and Enhanced BasicCards:

```
Call StartEncryption (P1=algorithm, P2=keynum, Rnd)
Call EndEncryption()
```

Professional BasicCard:

```
Call ProEncryption (P1=algorithm, P2=keynum, Rnd, Rnd)
Call EndEncryption()
```

That's all you have to do. An example program is provided in **8.9 Encryption – a Worked Example**.

The program running in the BasicCard will usually want to know whether encryption is currently in force. It can check this through the pre-defined variables **Algorithm** and **KeyNumber**, which contain the two parameters **P1** and **P2** that were passed in the most recent **StartEncryption** command. If encryption is not in force, both these variables have the value zero.

3.17.2 Key Declaration

The **Declare Key** statement declares a cryptographic key (the **KEYGEN** program outputs its keys as **Declare Key** statements in the key file):

Declare Key *keynum* [(*length* [, *counter*])] [= *b1*, *b2*, *b3*, . . .]

keynum The key number, by which the key can be specified (for example, in a **StartEncryption** command). It can take any value from 0 to 255, except in Enhanced BasicCard programs, where 255 is not allowed.

length The length of the key. If absent, the key length defaults to 8 bytes. If an initial value field (*b1*, *b2*, *b3*, . . .) is present, and no length is specified, the key length is set to the number of bytes in the initial value field. (If the length is specified, the initial value field is padded with zeroes to the required length.)

Note: In the Compact BasicCard, all keys must be 8 bytes long.

counter The error counter for the key (0 ≤ *counter* ≤ 15). If *counter* is zero, the key is initially disabled. If *counter* is absent, the error counter for the key is initially inactive. See **3.17.5 Key Error Counter** for details.

Note: the *counter* parameter is allowed in all programs, but it is ignored in Terminal programs and Compact BasicCard programs. This allows the same key file to be used in all programs in an application.

3. The ZC-Basic Language

b1, b2, b3, . . . The initial value of the key. If no initial value is provided, the key is initialised to zeroes. The key may be changed later, in one of three ways:

- with **Key(keynum) = string**, except in a Compact BasicCard program (see **3.16.4 Encryption Functions**);
- with the **Read Key File** statement in a Terminal program (see **3.17.4 Run-Time Key Configuration**);
- with the **BCKEYS** program in a Compact or Enhanced BasicCard (see **5.9.5 The Key Loader BCKEYS.EXE**).

Note: **Triple DES** and **AES-128** encryption require 16-byte keys; **AES-192** and **AES-256** encryption require 24-byte and 32-byte keys respectively.

3.17.3 Polynomial Declaration

The encryption algorithm described in **8.6 The SG-LFSR Algorithm** requires two primitive polynomials, of degree 31 and 32. (This is the encryption algorithm used by the Compact BasicCard.) You don't need to know what a primitive polynomial is, because the **KEYGEN** program generates them for you, and outputs them to the key file as a **Declare Polynomials** statement:

Declare Polynomials = PolyA&, PolyS&

PolyA& A primitive polynomial of degree 31, the generator of the Linear Feedback Shift Register **A**.

PolyS& A primitive polynomial of degree 32, the generator of the Linear Feedback Shift Register **S**.

The polynomials may be initialised at compile time, or later – with the **Read Key File** statement in a Terminal program, or with the **BCKEYS** program in a BasicCard.

3.17.4 Run-Time Key Configuration

The Terminal program can load keys and/or polynomials from a key file at run-time, with the statement

Read Key File *filename*

If this command fails, the File System variable **FileError** contains a non-zero error code indicating the reason for the failure – see **4.12 The Definition File FILEIO.DEF** for a list of error codes.

Except in Compact BasicCard programs, keys can also be accessed as strings via the **Key(keynum)** function. See **3.16.4 Encryption Functions** for details.

3.17.5 Key Error Counter

In the Enhanced and Professional BasicCards, each cryptographic key has an error counter. If the error counter for a particular key is active, it limits the number of times that a Terminal program can attempt to guess the key. For example, suppose the error counter for key *keynum* has an initial value of 10. Whenever the BasicCard receives a command that is encrypted with key *keynum*:

- if the encryption is invalid, the error counter is decremented, and the BasicCard returns the status code **SW1-SW2 = swRetriesRemaining+X** (&H63C0+X), where *X* is the new value of the error counter. When the error counter reaches zero the key is disabled, until an **Enable Key** command is executed in the BasicCard program (see below);
- if the encryption is valid, the error counter is reset to its initial value (in this case, 10);
- if the key is disabled (i.e. the error counter is already zero), the BasicCard responds with status code **SW1-SW2 = swKeyDisabled** (&H6614).

So the Terminal program is given 10 chances, after which no more commands encrypted with key *keynum* are accepted.

In an Enhanced or Professional BasicCard program, two commands are available for setting a key's error counter:

Enable Key *keynum* [(*counter*)]

Enables the key. If *counter* is present, the error counter for the key is activated, and its initial value is set to **Max** (*counter*, 15). If *counter* is absent, or equal to 255, the error counter for the key is deactivated (i.e. the key will remain enabled regardless of how many times a command is badly encrypted with the key).

Disable Key *keynum*

Disables the key, until a subsequent **Enable Key** command is executed.

Note: This error counter mechanism only applies to the encryption of commands. Even if a key is disabled, it can always be used from within a BasicCard program. ZC-Basic functions that use cryptographic keys are listed in **3.16.4 Encryption Functions**.

3.17.6 DES Encryption Primitives

DES message encryption and decryption is based on the four block encryption primitives E_K , D_K , E_K^3 , and D_K^3 , as defined in **8.1 The DES Algorithm**. In a Terminal program, an Enhanced BasicCard, and a Professional BasicCard with **DES** support, these primitives are available to the ZC-Basic programmer via the **DES** function:

result\$ = **DES**(*type*, *key*, *block\$*)

type The type of primitive: +1, -1, +3, or -3, as follows:

+1:	$E_K(block)$	Single DES encryption
-1:	$D_K(block)$	Single DES decryption
+3:	$E_K^3(block)$	Triple DES encryption
-3:	$D_K^3(block)$	Triple DES decryption

key Either a key number from 0 to 255, or a string containing a cryptographic key. The key must be at least 8 bytes long for types +1 and -1, and at least 16 bytes long for types +3 and -3.

block\$ An 8-byte string containing the block to encrypt or decrypt. If longer than 8 bytes, only the first 8 bytes are used; if shorter than 8 bytes, P-Code error **pcBadStringCall** (&H0D) is generated.

result\$ The 8-byte result of the DES encryption or decryption function.

3.17.7 Certificate Generation

The Terminal program, Enhanced BasicCards, and Professional BasicCards with **DES** support can generate “digital certificates” using cryptographic keys. A digital certificate is an electronic verification of a piece of data. Suppose you have a network of dealers, who can unload cash credits from the cards that you issue to your customers, in return for goods and services that they provide. At the end of the week, they come to you to exchange these electronic cash credits for real money. How can you be sure that the dealers are honest?

Digital certificates are the answer. To unload credits from a customer’s card, the dealer sends a message saying “I am dealer number *A*, and I want *B* credits”. The customer’s BasicCard will have its own ID number *C*, and it can maintain a transaction counter *D*, which it increments after each transaction. The BasicCard program puts these four numbers *A*, *B*, *C*, and *D* together into a string or a user-defined variable, and generates a certificate using a secret key not known to the dealer or the customer. This certificate is then returned to the dealer, who shows it to you to claim reimbursement for the credits. You can write a Terminal program to check that *A*, *B*, *C*, and *D* really do generate the correct certificate with the secret key. And because the key is known only to you and the BasicCard, you know that the dealer hasn’t forged the certificate.

To generate a certificate:

S\$ = **Certificate**(*key*, *data*)

where *key* is a key number from 0 to 255 or a string containing a cryptographic key, and *data* is the data to be verified – either an expression of type **String**, or a fixed-length variable or array element. This generates a **Triple DES** certificate if key number *key* is 16 bytes or longer, otherwise a **Single DES** certificate. The result, *S\$*, is always 8 bytes long. The certificate generation algorithm is described in **8.3 Certificate Generation Using DES**.

3. The ZC-Basic Language

3.18 Random Number Generation

The **Rnd** built-in function returns a 4-byte random number. The Terminal and the various BasicCards have different mechanisms for random number generation.

3.18.1 The Terminal

The Terminal program initialises its random number generator with a seed based on the system clock. This ensures that the **Rnd** function returns a different sequence every time a program runs. You can override this behaviour with the **Randomize** command:

Randomize *seed*

where *seed* is any expression of type **Long** or **String**.

You might want to do this for the following reasons:

- to generate a predictable sequence of random numbers while developing a program, to make debugging easier;
- to use a more unpredictable seed than the system clock, for better security.

Note: The default behaviour of the random number generator is good enough for the encryption algorithms used in communication with the BasicCard – these algorithms don't depend critically on the unpredictability of the initial values **RA** and **RB** (see **7.7.10 The START ENCRYPTION Command** for details). However, they do depend critically on the secrecy of the keys used, and for this purpose we provide a high-quality random number generation mechanism in the **KEYGEN** program (see **5.9.4 The Key Generator KEYGEN.EXE**).

3.18.2 The Compact and Enhanced BasicCards

Each Compact and Enhanced BasicCard has a unique serial number burnt into its memory. The first time in its life that the BasicCard generates a random number, this serial number is used as the seed. The seed is then updated and stored in EEPROM for the next random number generation. This ensures that:

- each BasicCard generates a different sequence of random numbers;
- a given BasicCard doesn't generate the same sequence each time it is reset.

The **Randomize** command is not available in the BasicCard.

Note: The BasicCard simulators in the **ZCMSIM** and **ZCMD CARD** programs do generate the same sequence of random numbers each time they run. This is because they have no access to a unique serial number to seed the generation mechanism. But when the program is downloaded to a genuine BasicCard, the random number sequence will become unpredictable.

3.18.3 The Professional BasicCard

All the Professional BasicCards have a hardware random number generator, so the **Rnd** function returns a truly random number.

3.19 Error Handling

If the P-Code interpreter in the BasicCard detects a run-time error, such as arithmetic overflow or insufficient memory, it calls the **ErrorHandler** procedure. If there is no procedure with this name in the program, it exits with the status code **SW1 = sw1PCCodeError** (&H64). **SW2** contains the P-Code error code (see **7.6.2 BasicCard P-Code Interpreter** for a list of these error codes). The **ErrorHandler** procedure may perform clean-up operations, but it cannot cause execution to be resumed at the statement that caused the error. The pre-defined variable **PCCodeError** contains the P-Code error code.

In the Enhanced and Professional BasicCards, the address of the instruction where the error occurred is passed to the **ErrorHandler** procedure as an **Integer** parameter, so you can access it by declaring e.g.

Sub ErrorHandler (PC As Integer)

3.20 BasicCard-Specific Features

3.20.1 Customised ATR

When the BasicCard is reset, it provides information about itself by means of the **ATR** (Answer To Reset). The **ATR** contains technical information about the communication parameters that the card uses, followed by up to fifteen bytes (the ‘Historical Characters’) by which the card can identify itself. The Historical Characters in the BasicCard are of the form “**BasicCard ZC_{vvv}**”, where *vvv* is the firmware version number of the card. You can supply your own Historical Characters with the **Declare ATR** statement:

Declare ATR = data

data Any sequence of **Byte** and **String** constants, with a total length <= 15.

You can specify the whole of the ATR (and not just the Historical Characters) with the statement

Declare Binary ATR = data

Here *data* must have a total length <= 31. Unless you know exactly what you are doing, you should only use this statement with data supplied by ZeitControl.

3.20.2 Application ID

The BasicCard has a pre-defined command **GET APPLICATION ID** (see **7.7.9 The GET APPLICATION ID Command**). You can use this command to check that the BasicCard in the card reader contains your application. To configure an Application ID:

Declare ApplicationID = data

data Any sequence of **Byte** and **String** constants, with a total length <= 127.

3.20.3 Enabling and Disabling Encryption Algorithms

{**Enable** | **Disable**} **Encryption** [*AlgorithmID* [, *AlgorithmID*, . . .]]

AlgorithmID The ID of an encryption algorithm. If no algorithm is specified, all available algorithms are enabled or disabled. The following algorithm IDs are available:

Compact BasicCard:	&H11	SG-LFSR
	&H12	SG-LFSR with CRC-16
Enhanced BasicCard:	&H21	Single DES
	&H22	Triple DES
Professional BasicCard:	&H23	Single DES with CRC-32
	&H24	Triple DES with CRC-32
	&H31	AES-128
	&H32	AES-192
	&H33	AES-256

For maximum security, you should disable any encryption algorithms that you don’t plan to use.

Notes:

- This command is executed when the program is compiled, and it lasts for the lifetime of the card. Algorithms can’t be enabled or disabled at run-time.
- Different Professional BasicCards support different combinations of the above five algorithms.

3.20.4 Asking the Terminal for More Time

The BasicCard has a **BWT** (Block Waiting Time) of 1.6 seconds (Compact) or 12.8 seconds (Enhanced and Professional) – see **7.4 The T=1 Protocol** for more information. If a command is going to take longer than this to complete, it must request more time, otherwise the caller will time out (but see **3.21.9 Giving the Card More Time**). It does this with a **WTX** (Waiting Time Extension) statement:

WTX *BWT-units*

3. The ZC-Basic Language

BWT-units Any expression of type **Byte**: the number of multiples of **BWT** requested. **WTX** requests are not cumulative – each request cancels all previous requests. *Note*: Some card readers treat 255 as a special value. If in doubt, don't use this value – use 254 instead.

In the **T=0** protocol, the *BWT-units* parameter is ignored, and a single **NULL** byte (&H60) is sent. This resets the **WWT** (Work Waiting Time) time-out period – see **7.3 The T=0 Protocol** for more information.

3.20.5 Pre-Defined Variables

The BasicCard operating system has a number of internal variables that can be accessed from the ZC-Basic language. Most of these have to do with communications – see **Chapter 7: Communications** for details. The following are all **Public** variables (in RAM) of type **Byte**:

CLA	Class byte – first byte of two-byte CLA INS command identifier.
INS	Instruction byte – second byte of two-byte CLA INS command identifier.
P1	Parameter 1 of 4-byte CLA INS P1 P2 command header.
P2	Parameter 2 of 4-byte CLA INS P1 P2 command header.
Lc	Length of IDATA field in command.
Le	Expected length of ODATA field in response (supplied by caller).
ResponseLength	Actual length of ODATA field in response (supplied by called command).
SW1	First status byte in response field SW1-SW2 .
SW2	Second status byte in response field SW1-SW2 .
Algorithm	ID of currently active encryption algorithm. Commands can check this byte to ascertain whether an appropriate encryption mechanism is in force. If no encryption is currently active, Algorithm is zero. See 3.20.3 Enabling and Disabling Encryption Algorithms for a list of algorithm IDs.
KeyNumber	The number of the cryptographic key being used by the currently active encryption algorithm. If no encryption is currently active, KeyNumber is zero (but zero is also a valid key number, so you should not use KeyNumber to check whether encryption is active – use Algorithm for this purpose).
PCodeError	If a run-time error occurs, and the program contains a subroutine with the name ErrorHandler , then this subroutine is called. The error code is available to the ErrorHandler subroutine in the variable PCodeError .
FileError	The most recent error code generated by the file system (Enhanced and Professional BasicCards only).
LibError	The most recent library procedure error (only the Professional BasicCard pre-defines this variable – an Enhanced BasicCard program declares it in the <i>library.def</i> file).

Two **Integer** variables are defined:

P1P2	Concatenation of P1 and P2 .
SW1SW2	Concatenation of SW1 and SW2 .

3.21 Terminal-Specific Features

3.21.1 Screen Output

Screen output uses the **Cls** and **Print** statements in conjunction with the four pre-defined variables **FgCol**, **BgCol**, **CursorX**, and **CursorY** (see **3.21.10 Pre-Defined Variables**).

The **Cls** command clears the screen, and sets **CursorX** and **CursorY** to 1:

Cls

The **Print** statement:

Print [*field* | *separator*] [*field* | *separator*] . . .

<i>field</i>	Any Byte , Integer , Long , Single , or String expression
<i>separator</i>	‘;’ (semi-colon) Leaves the output column unchanged. ‘,’ (comma) Advances the output column to the next output field (an output field is 14 characters wide). Spc (<i>n</i>) Prints <i>n</i> space characters. Tab (<i>n</i>) Advances the output column to position <i>n</i> .

After the print statement, the cursor advances to the start of the next line, unless the last character is a separator. (So you can stay on the same output line by adding a semi-colon at the end of the command.)

3.21.2 Keyboard Input

InKey\$	Returns a string containing 0, 1, or 2 bytes: 0 bytes if there is no character waiting in the keyboard buffer; 1 if a regular key was pressed; 2 if an extended-ASCII key was pressed (in which case the first byte is zero).
Line Input X\$	Reads a line from the keyboard into the string variable X\$, until the carriage return key is pressed.
Input variable-list	Reads the variables in the list from the keyboard. If the list contains more than one variable, the user must separate the values with commas or spaces. This statement can also appear on the right-hand side of an assignment statement:

n = **Input** *variable-list*

This returns the number of variables in the list that were successfully input.

3.21.3 Communications

Three functions are provided for determining the status of the card reader and card. These functions return a status code in **SW1**–**SW2**, just like command calls:

CardReader [(*name\$*)]

Attempts to detect a card reader via the configured serial port. If a string parameter is passed, the identification string of the card reader is returned. If the BasicCard is being simulated in the PC, the words “Simulated Card Reader” are returned in the *name\$* parameter.

Status Codes in SW1-SW2:

swCommandOK	Card reader detected
swNoCardReader	Card reader not detected
swCardReaderError	Invalid response from card reader

CardInReader

Returns **swCommandOK** (&H9000) if a card is in the card reader.

Status Codes in SW1-SW2:

swCommandOK	Card is in card reader
swNoCardReader	Card reader not detected
swCardReaderError	Invalid response from card reader
swNoCardInReader	No card in reader

ResetCard [(*ATR\$*)]

Attempts to reset the card, returning **swCommandOK** (&H9000) if the card responded with a valid Answer To Reset. If a string parameter is passed, the Historical Bytes of the Answer To Reset are returned. See also **3.20.1 Customised ATR**.

Status Codes in SW1-SW2:

swCommandOK	Valid Answer To Reset received
--------------------	--------------------------------

3. The ZC-Basic Language

swNoCardReader	Card reader not detected
swCardReaderError	Invalid response from card reader
swNoCardInReader	No card in reader
swT1Error	T=1 protocol error (see 7.4 The T=1 Protocol)
swCardError	Invalid response from card
swCardTimedOut	Card failed to send an ATR within the prescribed time

3.21.4 PC/SC Functions

Two functions are provided for obtaining information about the PC/SC-compatible card readers configured in the system:

nReaders = PcscCount

Returns the number of configured PC/SC card readers, as an **Integer**.

Status codes in SW1-SW2:

swNoPcscDriver	The PC/SC driver is not installed in the system.
swPcscError	The PC/SC driver returned an unexpected error code.

ReaderName = PcscReader(ReaderNum)

Returns the name of PC/SC card reader *ReaderNum*, as a **String**. If *ReaderNum* is zero, the name of the default PC/SC reader is returned. To access PC/SC reader number *ReaderNum*, set the pre-defined variable **ComPort** to *ReaderNum*+100.

Status codes in SW1-SW2:

swNoCardReader	<i>ReaderNum</i> is less than zero or greater than <i>nReaders</i> .
swNoPcscDriver	The PC/SC driver is not installed in the system.
swPcscError	The PC/SC driver returned an unexpected error code.

Note: To configure a default PC/SC reader, add the reader's name to the Windows® system registry, in the field "HKEY_CURRENT_USER\Software\ZeitControl\BCPCSC\Default" (you can do this with the Windows system tool Regedit.Exe). If no such field is found, reader number 1 is the default.

3.21.5 I/O Logging

The **Open Log File** statement initiates the logging of all I/O between the Terminal program and the BasicCard program:

Open Log File *filename*

Previous contents of the log file are destroyed. If the file open fails, the pre-defined variable **FileError** is set to a non-zero value – see **4.12 The Definition File FILEIO.DEF** for error codes. The statement

Close Log File

ends I/O logging and closes the log file.

3.21.6 Date and Time

The string function **Time\$** returns a 24-character string containing the current date and time in fixed format:

"Ddd Mmm DD HH:MM:SS YYYY" (for example: **"Wed Jun 24 15:50:35 1998"**).

3.21.7 Saving Eeprom Data

The statement

Write Eeprom [(*filename*)]

writes the permanent **Eeprom** data in the Terminal program to a disk file. If *filename* is not given, the data is written back to the original image file (or debug file). If the file couldn't be opened for any reason, the pre-defined variable **FileError** is set to a non-zero value – see **4.12 The Definition File FILEIO.DEF** for a list of error codes.

Note: The **Write Eeprom** statement is only valid if the Terminal program is running in the **ZCMSIM** P-Code interpreter or the **ZCMDTERM** Terminal Program debugger. Programs containing **Write Eeprom** statements can't be compiled into executable files.

3.21.8 Automatic Encryption

{ **Enable** | **Disable** } **Encryption**

The P-Code interpreter that runs the Terminal program monitors all commands to the BasicCard, watching for **START ENCRYPTION** and **END ENCRYPTION** commands. If it sees a well-formed **START ENCRYPTION** command that receives a valid response from the BasicCard, it automatically turns on encryption of commands and decryption of responses, until it sees an **END ENCRYPTION** command. If for any reason you want to disable this monitor, you can do it with a **Disable Encryption** command. You can turn the monitor back on at any time with **Enable Encryption**.

3.21.9 Giving the Card More Time

Sometimes the BasicCard needs more than the Block Waiting Time to execute a command. In principle, the card is responsible for requesting more time, which it does with a **WTX** statement – see **3.20.4 Asking the Terminal for More Time**. However, if you have a ZeitControl Chipi® card reader, you can also override the default Block Waiting Time from the Terminal program with a **WTX** statement:

WTX *seconds*

seconds Any expression of type **Byte**: the number of seconds to give the card before timing out. Unlike **WTX** requests in the BasicCard program, this time-out value remains in effect until explicitly cancelled (by **WTX 0**). If *seconds* is equal to 255, the card is given unlimited time to respond.

The Terminal program waits for a response from the card until *both* time-outs (those set by the BasicCard program and the Terminal program) have expired.

Note: This feature is only available if **ComPort** ≤ 4, and you are accessing a ZeitControl Chipi® card reader via the serial port. The PC/SC standard interface, and the CyberMouse® card reader, do not support this feature. See **3.3.11 Block Waiting Time** for an alternative method of increasing time-outs.

3.21.10 Pre-Defined Variables

The Terminal P-Code interpreter contains the following **Public** pre-defined variables, of type **Byte**:

ComPort The number of the COM port that the card reader is attached to. To specify PC/SC card reader number *n*, set **ComPort** = *n*+100 (or **ComPort** = 100 for the default PC/SC reader – see **3.21.4 PC/SC Functions** for details).

Note: The value of **ComPort** at program start-up is taken from the environment variable **ZCPORT**, if it exists; otherwise the Windows Registry variable **ZCPORT** in the directory **HKEY_CURRENT_USER\Software\ZeitControl\BasicCardPro**, if it exists; otherwise it takes the value 1.

ResponseLength The length of the **ODATA** field in the last response received from the card.

SW1 First byte of **SW1-SW2** status field in the last response received from the card.

SW2 Second byte of **SW1-SW2** status field in the last response received from the card.

Algorithm ID of currently active encryption algorithm. Commands can check this byte to ascertain whether the appropriate encryption mechanism is in force. If no encryption is currently active, **Algorithm** is zero. See **3.20.3 Enabling and Disabling Encryption Algorithms** for a list of algorithm IDs.

KeyNumber The number of the cryptographic key being used by the currently active encryption algorithm. If no encryption is currently active, **KeyNumber** is zero (but zero is also a valid key number, so you should not use **KeyNumber** to check whether encryption is active – use **Algorithm** for this purpose).

3. The ZC-Basic Language

PCodeError	If a run-time error occurs, and the program contains a subroutine with the name ErrorHandler , then this subroutine is called. The error code is available to the ErrorHandler subroutine in the variable PCodeError .
FgCol	Foreground colour for Print statements to the screen (0-15).
BgCol	Background colour for Print statements to the screen (0-15).
CursorX	X-coordinate of text cursor (1-80).
CursorY	Y-coordinate of text cursor (1-25).
FileError	The most recent error code generated by a file I/O operation.
nParams	Number of command-line parameters (see 5.9.2 The P-Code Interpreter ZCMSIM.EXE).

One **Integer** variable is defined:

SW1SW2 Concatenation of **SW1** and **SW2**.

Two **String** arrays are defined:

Param\$(1 To nParams) Command-line parameters passed to the **ZCDOS** program (see **5.9.2 The P-Code Interpreter ZCMSIM.EXE**).

Key(0 To 255) Cryptographic keys.

3.22 Miscellaneous Features

This section lists all the ZC-Basic statements that are not covered in the preceding sections or in **Chapter 4: Files and Directories**.

3.22.1 Overflow Checking

{ **Enable** | **Disable** } **OverflowCheck**

Normally, if the result of an arithmetic operation is too big or too small to be represented in the target type, a P-Code error is generated. You can enable or disable this overflow checking with **Enable OverflowCheck** or **Disable OverflowCheck**. These statements are executed at run-time, and don't apply to the whole program. (So if you want to disable overflow checking for the whole program, then **Disable OverflowCheck** should appear in your initialisation code.)

Note: This statement only affects whole-number arithmetic (**Byte**, **Integer**, and **Long** data types). Floating-point overflow checking (**Single** data type) cannot be turned off.

3.22.2 DefType Statement

A **DefType** statement specifies the default type of variables, arrays, and functions that begin with a certain letter or range of letters:

{ **DefByte** | **DefInt** | **DefLng** | **DefSng** | **DefString** } *range* [, *range*, ...]

range Either a single letter, or a range of letters separated by a minus sign (e.g. **I-N**). The case of the letter(s) is not significant.

The initial setting is **DefInt A-Z**, i.e. all variables, arrays, and functions have type **Integer** by default.

3.22.3 Array Subscript Base

An array subscript range takes the form

[*lower-bound* **To** *upper-bound*]

If the optional *lower-bound* is missing, it defaults to **0**. You can change this default value with the **Option Base** command, which applies to all subsequent array declarations:

Option Base *subscript-base*

subscript-base Any constant expression. In the Compact and Enhanced BasicCards, it must satisfy $-32 \leq \text{subscript-base} \leq +31$.

Or you can specify that the lower bounds of array subscripts must always be explicitly declared, with

Option Base Explicit

3.22.4 Explicit Declaration of Variables and Arrays

By default, ZC-Basic allows implicit declaration of variables and arrays:

- If it meets a variable that it doesn't recognise in an expression or an assignment statement, it will treat it as a newly-declared variable. The type of the variable is determined from its name, as described in **3.7 Data Declaration**.
- If a **ReDim** statement contains an unrecognised array name, the compiler inserts an implicit **Dim** statement to declare the array.

The Basic programming language has always behaved this way. However, this can be dangerous, as it accepts mis-typed variable names as new variables. In the following example, this results in **TransactionState** ending with the value **1** instead of **13**:

```
TransactionState = 12
...
TransactionState = TransatcionState + 1
```

You can catch all such errors by using the **Option Explicit** statement:

Option Explicit

This tells the compiler not to accept variables or array names that haven't been explicitly declared. It applies only to following code; preceding code can contain implicit declarations.

3.23 Technical Notes

3.23.1 Parameter Size Limits

The maximum total size of all the parameters in a procedure call is approximately 128 bytes. More precisely, the compiler checks that the sum of the following contributions is ≤ 128 :

- the total size of all the fixed-length parameters (including **String*n**);
- 2 bytes for each parameter of array type;
- 3 bytes for each **String** parameter (or 2 bytes for the final **String** parameter to a **Command**);
- for a **Function**, the size of the return value (2 bytes if this is a **String**);
- 2 bytes for the return address (unless it's a **Command**);
- the frame overhead (2 bytes for the Compact and Enhanced BasicCards, otherwise 4 bytes).

See also Note 4 in **3.12.3 Command** for more on the final **String** parameter to a **Command**.

3.23.2 Array Descriptor Format

An array in ZC-Basic consists of a fixed-length *array descriptor*, and a *data area* (which is of variable length if the array is **Dynamic**). In a Compact or Enhanced BasicCard program, if an array has **n** dimensions, then its descriptor occupies $2*n + 4$ bytes:

Address of data area (0 if not allocated) (2 bytes)			
Size of each element (1 byte)	D	n (7 bits)	
LO(1) (6 bits)	RANGE(1) (10 bits)		
...	...		
LO(n) (6 bits)	RANGE(n) (10 bits)		

D This bit is **1** for **Dynamic** arrays, **0** for **Fixed** arrays.
LO(i) Lower bound for subscript(i): $-32 \leq \text{LO}(i) \leq 31$.
RANGE(i) Range for subscript(i): $0 \leq \text{RANGE}(i) \leq 1023$.

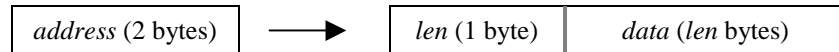
3. The ZC-Basic Language

The upper bound of subscript(*i*) is equal to **LO**(*i*) + **RANGE**(*i*).

In Terminal programs and Professional BasicCard programs, **LO**(*i*) and **HI**(*i*) are 2-byte integers, so the descriptor occupies **4*n + 4** bytes.

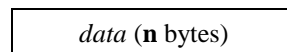
3.23.3 String Parameter Format

A variable of type **String** is a 2-byte pointer to a (*len*, *data*) pair:



This uses *len*+3 bytes of storage (but if *len* is zero, then *address* is zero too, so only 2 bytes are used).

A variable of type **String*n** requires just *n* bytes of storage:



A procedure parameter of type **String*n** also takes up *n* bytes on the P-Code stack.

However, a procedure parameter of type **String** is rather more complicated. Two requirements must be fulfilled:

- A procedure can change the value of a **String** variable passed as a parameter;
- A **String*n** variable can be passed as a **String** parameter.

So a **String** parameter takes up 3 bytes on the P-Code stack. If a fixed-length **String*n** variable was passed, then the first of these bytes contains the length *n* (0-254) and the next two bytes contain the address of the data. Otherwise, the first byte contains 255 (**&HFF**) and the next two bytes contain the address of the pointer (not the address of the data). So if the address of the data has to be changed because the string increases in length, the **String** variable can be updated to point to the new data. (By the way, this is the reason for the 254-byte length restriction on all strings.)

3.23.4 Memory Allocation in the BasicCard

The ZC-Basic compiler calculates the sizes of all the memory regions in RAM and EEPROM. Any memory left over is assigned to the two heaps, **RAMHEAP** and **EEPHEAP**. These regions are for run-time memory allocation. (See **9.4 Run-Time Memory Allocation** for the format of the allocated memory blocks.)

The ZC-Basic P-Code interpreter uses run-time memory allocation for three kinds of data: variable-length **String** data, **Dynamic** arrays, and files. Files and **Eeprom** data are allocated as **Permanent** blocks in **EEPHEAP**. Other data is allocated in **RAMHEAP** if there is room, but if not, it is allocated as **Temporary** blocks in **EEPHEAP**. All **Temporary** blocks are freed the next time the BasicCard is reset or the Terminal program is started. EEPROM writes require up to 6 milliseconds to complete, so a BasicCard program runs more slowly when it has to use **EEPHEAP** in this way.

3.23.5 Single-to-String Conversion

The operating system in the Enhanced BasicCard consists of 17.7K of code; the chip, however, contains only 17K of ROM. The last 705 bytes contain the Single-to-String conversion routines. If an Enhanced BasicCard program requires these routines, the **ZCMBASIC** compiler automatically loads them into EEPROM (in the **STRVAL** region – see **9.1.2 The Enhanced BasicCard**). This means, of course, that the amount of EEPROM available for your code and data is reduced by 705 bytes.

If any of the following ZC-Basic statements occur in an Enhanced BasicCard program, this **STRVAL** region will be loaded:

- **Str\$(val)** with a *val* parameter of type **Single**;
- **Val!(string)** (**String** to **Single** conversion);
- **Print** to file, with a parameter of type **Single**.

Some versions of the Professional BasicCard do not support **Single-to-String** conversion – see the **Professional BasicCard Datasheet** for details.

4. Files and Directories

4.1 Directory-Based File Systems

Everybody who owns a PC is familiar with directory-based file systems. Each disk drive has a special directory, called the *root directory*, which contains data files and sub-directories. These sub-directories themselves can contain data files and sub-directories, and so on. This determines a tree of directories, in which any directory in the tree can contain data files and sub-directories. The directory containing a given data file or sub-directory is called its *parent* directory. (*directory* is the traditional term, which is used throughout this chapter; Windows[®] 98 calls its directories *folders*.)

4.1.1 File and Directory Names

Under Windows[®] 98, filenames can be up to 255 characters long, and may contain any printable character (including the space character), except the following:

\	Backslash	/	Slash	:	Colon	*	Asterisk
?	Question mark	"	Double quote	<	Left angle-bracket	>	Right angle-bracket
	Vertical bar						

Case is not significant when referring to an already existing file or directory. So if a file has the name "FILE.NAM", you can access it as "File.Nam" or "FiLe.nAm" or whatever. However, Windows[®] 98 retains the case of the characters specified when the file was originally named. So if you create a file as "File.Nam" and then ask for a directory listing, Windows[®] 98 lists it as "File.Nam".

4.1.2 Path Names

Each file and directory can be uniquely identified by a *full path name*. This consists of the disk drive name, followed by every sub-directory on the path from the root directory to the parent directory, followed by the name of the file or directory itself. The disk drive name is a letter A-Z followed by a colon, e.g. "C:" or "A:". (Lower-case letters may also be used to refer to disk drives, but a drive name returned by a ZC-Basic function will always be upper-case.) The drive name is immediately followed by a backslash character (this signifies the root directory); and subsequent directory names in the path are separated by backslash characters '\'. For example, a full path name might be "C:\1997 Clients\Account Data".

To save having to give the full path name every time, every disk drive in the system has a *current directory*, and the system as a whole has a *current drive*. If the disk drive name is missing from the front of a path name, the current drive is assumed. And if the first character after the disk drive name is not a backslash, then the chain of directories is followed starting from the current directory for the drive, instead of the root directory. Such a path name is called a *relative path name*. For instance, suppose the current drive is "C:", and the current directories for drives "A:" and "C:" are "\Clients.97" and "\Programs\CPP" respectively. Then the relative path names "A:August\TOTALS.DAT" and "Headers\SUM.H" expand to the full path names "A:\Clients.97\August\TOTALS.DAT" and "C:\Programs\CPP\Hheaders\SUM.H" respectively.

The directory names "." and ".." have special meanings: "." denotes the current position in the chain of directories, and ".." denotes the parent directory. So ".\" in a path has no effect, and "..\" goes back to the previous directory in the chain. For instance, in the previous example, the path name "..\Basic\FILEIO.BAS" expands to "C:\Programs\CPP\..\Basic\FILEIO.BAS", which is the same as "C:\Programs\Basic\FILEIO.BAS". The single-dot notation is useful when a directory is required as a parameter to a file system operation; for example, the ZC-Basic statement **Name "..\FileList" As ".\"** moves the file "FileList" from the parent directory to the current directory.

4.2 The BasicCard File System

The Enhanced and Professional BasicCards contain a directory-based file system, with the same file-naming rules as those described in the previous section for Windows® 98 (except that the maximum length of a full path name is 254 characters). The BasicCard has one root directory, so path names don't begin with a disk drive name. With the exception of the commands **CurDrive**, **ChDrive**, and **SetAttr**, the ZC-Basic file and directory commands available to a BasicCard program are the same as those available to a Terminal program.

4.2.1 File Access from a Terminal Program

If the BasicCard allows it, files and directories in the card can be accessed from a Terminal program, just as if the card was a diskette. The card has the special drive name "@:". Suppose the BasicCard contains a file "\Transport\Bus\Credits". Then the full path name of this file from the point of view of the Terminal program is "@:\Transport\Bus\Credits". And if the Terminal program sets the current drive to "@:" and the current directory to "\Transport", it can refer to the file as simply "Bus\Credits". The full range of file and directory commands is available to the Terminal program for accessing BasicCard files and directories, subject to appropriate access being granted.

Each file or directory in the BasicCard has its own access conditions, specifying the circumstances under which the Terminal program is allowed read and write access. These access conditions can be set and changed with **Lock** and **Unlock** statements. There are three types of access condition: **Read**, **Write**, and **Custom**. The following general rules apply to file and directory access:

- **Read** and **Write** access to all files and directories is available to the BasicCard program at all times.
- **Read** and **Write** access to all files and directories is available to the Terminal program as long as the BasicCard is in state **LOAD** or **PERS** (see 7.7.1 States of the BasicCard).
- Otherwise, to access a file or directory from the Terminal program, **Read** access is required to all directories in the path from the root to the parent. To delete a file or directory, or to change its access conditions, **Write** access is required to the file or directory, and to its parent directory. (In particular, when the card is in state **TEST** or **RUN**, the Terminal program can never change the root directory's access conditions, because the root directory has no parent.)
- If a **Custom** lock is placed on a file or directory, it is locked against **Read** and **Write** access every time the card is reset. It can only be unlocked from within the BasicCard program, after which the file's regular **Read** and **Write** access conditions apply until the next reset. So you can write a command that unlocks a particular file if the Terminal program sends the correct PIN number, for instance.

The **Read** and **Write** access conditions on a file or directory can be:

- **Allowed** – access is allowed from the Terminal program;
- **Forbidden** – access is forbidden from the Terminal program; or
- **Keyed** – access is allowed only if encryption with the appropriate key is enabled.

Read and **Write** access conditions and key numbers can be set independently of each other. If access is **Keyed**, up to two keys can be specified – if encryption with either of the two keys is enabled, access is allowed. The encryption algorithm must be **Triple DES** for keys at least 16 bytes long, and **Single DES** for shorter keys. So to access a **Keyed** file from a Terminal program, you must first call **StartEncryption** with the appropriate algorithm and key number – see 3.17.1 Implementing Encryption.

Note: The default access conditions on the root directory are **Read=Allowed** and **Write=Forbidden**.

4.2.2 Pre-Defined Files and Directories

In a BasicCard program, you can pre-define directories and data files using **Dir** and **File** statements. The compiler constructs the appropriate structures in EEPROM for downloading to the card. See 4.11 File Definition Section for details.

4.2.3 Storage Requirements

In the BasicCard, data files and directories are stored in EEPROM. To make efficient use of the limited space available, you should know how much memory is used. A data file or directory allocates space for its header and its name; a data file owns data blocks as well:

- A directory header requires 13 bytes of EEPROM; a data file header requires 19 bytes.
- The name of a file or directory takes up $n+2$ bytes of EEPROM, where n is the number of characters in the name.
- Each data block in a data file uses $n+4$ bytes of EEPROM, where n is the block length specified when the file was created. (The default block length is 32 bytes.) These blocks are allocated automatically when data is written to a file. *Note:* Contiguous data blocks are merged if they are also contiguous in EEPROM; this saves the overhead of 4 bytes per block. So if you are creating a file that is going to be written to just once, you can achieve optimum EEPROM usage by specifying a block length of 1 byte.

As well as these EEPROM requirements, the file system in the Enhanced BasicCard uses $(6 * nFiles + 7)$ bytes of RAM, where $nFiles$ is the number of open file slots configured (see **3.3.7 Number of Open File Slots**).

4.3 File System Commands

This chapter describes all the file system commands available to the ZC-Basic programmer. There are three cases that the ZC-Basic *interpreter* must distinguish:

1. A Terminal program accessing the file system in the PC (disk drives “A:” through “Z:”).
2. A Terminal program accessing the BasicCard file system (disk drive “@:”).
3. A BasicCard program accessing its own BasicCard file system (no disk drive).

However, these cases all look the same to the ZC-Basic *programmer*. Apart from the disk drive names, there are no differences, unless explicitly noted in the command descriptions that follow.

After each command, its required access conditions are listed. These access conditions apply only when the Terminal program attempts to access a file or directory in a BasicCard that is in state **TEST** or **RUN**.

All file system commands return a status byte in the pre-defined variable **FileError**. A zero value (**feFileOK**) indicates success. A non-zero value is an error code, and indicates the first error that occurred since this variable was last set to zero. (It is reset to zero every time a new command is received from the Terminal program; you may also set it to zero yourself if you want to continue after an error.) Error codes for each command are listed below.

As well as the error codes documented below under individual commands, there are some general error codes that apply to all commands:

feInvalidDrive	In cases 1 and 2 above (Terminal program), a disk drive name in a path was not a letter or “@:”.
feBadFilename	A filename contains an invalid character, or is too long (see 4.1.1 File and Directory Names).
feBadFilenum	A file number is out of range. In ZC-Basic, an open file is referred to by a file number. In a Terminal program, this number must be between 0 and 32 inclusive (with 0 indicating the screen or keyboard). In a BasicCard program, zero is not allowed; the maximum number allowed defaults to 2, but this can be overridden with a #Files directive (see 3.3.7 Number of Open File Slots).
feFileNotFound	A file or directory specified in a path name does not exist.
feFileNotOpen	The file number passed to the command is not associated with an open file. <i>Note:</i> This need not be the result of a programming error. If a Terminal program opens a file in the BasicCard, and then calls a BasicCard command,

4. Files and Directories

the BasicCard command can close all files unilaterally – including remotely-opened files – by using the **Close** command with no parameters. This is so that the BasicCard program can always find a free open file slot when it needs one.

feAccessDenied	The access conditions on a file or directory do not allow the execution of the command.
feBadFileChain	The file system in the BasicCard is corrupted.
feBadParameter	An invalid parameter value was passed to the command.
feOutOfMemory	The BasicCard has insufficient free EEPROM to execute the command.
feUnexpectedError	An operating system command in the PC returned an unexpected error code when a file system function was called.
feCommsError	In case 2 above (Terminal program accessing the BasicCard file system), the command failed because of a communications failure with the BasicCard. The status bytes describing the communications failure can be found in the pre-defined variables SW1 and SW2 .
feNoFileSystem	The card has no file system installed, either because <ul style="list-style-type: none">• it's a Compact BasicCard; or• no program has yet been downloaded to the card; or• the file system was disabled with a #Files 0 directive (see 3.3.7 Number of Open File Slots).

Definitions of these error codes, as well as all the other constants that appear in this chapter, are contained in the file **FILEIO.DEF**. This file is supplied in the distribution kit, and is listed in **4.12 The Definition File FILEIO.DEF**.

4.4 Directory Commands

4.4.1 Creating a Directory

The **MkDir** command creates a new directory (but see also **4.11 File Definition Sections**):

MkDir *path*

path The path name of the new directory. A final backslash '****' is optional.

Access Conditions:

Write access to the parent directory is required. The **Read** and **Write** access conditions of the new directory are the same as those of the parent directory.

Error Codes:

feFileNotFound	The parent directory does not exist.
feFileAlreadyExists	A file or directory with the given path name already exists.
feNameTooLong	The full path name of the directory would be longer than 254 characters.

4.4.2 Deleting a Directory

The **Rmdir** command deletes an existing directory. The directory must be empty before it can be deleted:

Rmdir *path*

path The path name of the directory. A final backslash '****' is optional.

Access Conditions:

Write access is required, both to the directory and to its parent directory.

Error Codes:

feFileNotFound	The directory does not exist.
feNotDirectory	The file is a data file, not a directory. Use Kill to delete data files.
feDirNotEmpty	The directory is not empty, and therefore can't be deleted.

4.4.3 Setting the Current Directory

The **ChDir** command sets the current directory.

ChDir *path*

path The path name of the new current directory. A final backslash '\' is optional.

Note (Terminal programs only): If the path contains a disk drive name, the current directory for that disk drive is changed, but the current disk drive is *not* changed. Use **ChDrive** to change the current disk drive.

Access Conditions:

Read access to the directory is required.

Error Codes:

feFileNotFound	The directory does not exist.
feNotDirectory	The file is a data file, not a directory.

4.4.4 Retrieving the Current Directory

The **CurDir** function returns the path of the current directory as a **String**:

S\$ = **CurDir** [(*drive*)]

drive The disk drive for which the current directory is requested. The first character must be a letter ('A-Z' or 'a-z'), or the character '@'. If absent, the current directory of the current disk drive is returned.

Note: The optional *drive* parameter is accepted only in Terminal programs.

Access Conditions:

No access conditions are required for this command.

Error Codes:

feInvalidDrive	The disk drive specified in the <i>drive</i> parameter does not exist.
feNameTooLong	The full path name of the current directory is longer than 254 characters (Terminal program only).

4.4.5 Renaming a File or Directory

The **Name** command renames a file or directory, or moves it to a new directory, or both. It cannot be used to move a file from one disk drive to another.

Name *OldPath* **As** *NewPath*

OldPath The old path name of the file or directory.

NewPath The new path name. If no backslash appears in *NewPath*, the file or directory is renamed without being moved. If *NewPath* ends with a backslash character '\', the file or directory is moved without being renamed.

Note: Under MS-DOS®, directories can be renamed, but not moved.

Access Conditions:

Write access is required (i) to the file or directory being renamed, (ii) to its parent directory, and (iii) to the destination directory if different from the current parent directory.

4. Files and Directories

Error Codes:

feFileNotFound	The file specified in <i>OldPath</i> does not exist, or the directory specified in <i>NewPath</i> does not exist.
feFileAlreadyExists	The file specified in <i>NewPath</i> already exists.
feNameTooLong	The operation would result in a file or directory in the BasicCard with a full path name longer than 254 bytes.
feRenameError	One of the following error conditions: <ul style="list-style-type: none">• <i>OldPath</i> is the root directory, which cannot be renamed.• <i>NewPath</i> and <i>OldPath</i> are on different disk drives.• An attempt was made to move a directory under MS-DOS®.
feRecursiveRename	The directory in <i>NewPath</i> is a sub-directory of <i>OldPath</i> , so the rename operation would result in an endless loop in the directory tree.

4.4.6 Searching for Files

Use the **Dir** command to search for files and directories matching a given wild-card specification. This has two forms:

nFiles = **Dir** (*filespec*) Returns the number of matching files and directories, as an **Integer**.

file\$ = **Dir** (*filespec*, *n*) Returns the name of the *n*th matching file or directory, as a **String**.

filespec The path name of the file(s) to search for. The last component of the path may contain the wild-card characters '?' (matching any single character) and '*' (matching any sequence of zero or more characters). For example, "A*" finds all filenames that start with the character 'A' or 'a', and "*=?" finds all filenames whose penultimate character is '='.

n The number of the matching file, $1 \leq n \leq nFiles$.

Notes:

1. If *filespec* refers to a file or files in the PC, the first **Dir** command for a given *filespec* saves all the matching files in memory. This list is retained for future **Dir** commands of the second form that have the same *filespec* parameter (unless a ZC-Basic command intervenes that can change the directory contents). This is a major speed improvement in most cases. However, if another process changes the directory contents, ZC-Basic won't know about it, and will continue to use the original list. You can override this at any time and re-load the list from the disk, by calling a **Dir** command of the first form.
2. ZC-Basic uses the host operating system to match wild-card specifications in the PC. MS-DOS® and Windows® 98 handle wild-card characters a little differently, due to the differences in what constitutes a valid filename, but "* . *" matches all files and directories in both systems.
3. The Enhanced BasicCard uses a case-insensitive matching algorithm that treats the full stop (period) character '.' no differently from any other character (unlike MS-DOS® and Windows® 98). However, as a special case, the wild-card string "* . *" matches all files and directories.

Access Conditions:

Read access to the parent directory is required.

Error Codes:

feBadFilename	<i>filespec</i> is not a valid path name (this error code is also returned if <i>filespec</i> contains wild-card characters in any component except the last).
feBadFilenum	<i>n</i> is less than 1 or greater than <i>nFiles</i> .

4.4.7 Setting the Attributes of a File or Directory

The **SetAttr** command sets the attributes of a file or directory:

SetAttr *filename, attributes*

<i>filename</i>	The path name of the file or directory.
<i>attributes</i>	A bit map of the attributes to set. The attributes available depend on the host operating system. See 4.4.8 Retrieving the Attributes of a File or Directory for details.

Note: This command is available in Terminal programs only.

Access Conditions:

Access conditions are not relevant for this command, as a BasicCard file has no attributes that can be changed.

Error Codes:

feRemoteFile *filename* is a BasicCard file, so it has no attributes that can be changed.

4.4.8 Retrieving the Attributes of a File or Directory

The **GetAttr** command returns the attributes of a file or directory:

attributes = **GetAttr** (*filename*)

<i>filename</i>	The path name of the file or directory.																
<i>attributes</i>	A bit map of the attributes of the file or directory. The attributes that can be returned depend on the host operating system, as follows: <ul style="list-style-type: none"> The BasicCard file system supports two attributes: <table> <tr> <td>faDirectory</td><td>Indicates that the file is a directory, and not a data file.</td></tr> <tr> <td>faCardFile</td><td>Indicates that the file or directory is in the BasicCard.</td></tr> </table> MS-DOS[®] supports these two attributes, plus the following: <table> <tr> <td>faReadOnly</td><td>Indicates a read-only file.</td></tr> <tr> <td>faHiddenFile</td><td>Indicates a hidden file.</td></tr> <tr> <td>faSystemFile</td><td>Indicates a system file.</td></tr> <tr> <td>faArchived</td><td>Indicates that file has been backed up since last changed.</td></tr> </table> Windows[®] 95 supports all the above attributes, plus the following: <table> <tr> <td>faNormal</td><td>Indicates that no other attribute bits are set.</td></tr> <tr> <td>faTemporary</td><td>Indicates that file is being used for temporary storage.</td></tr> </table> 	faDirectory	Indicates that the file is a directory, and not a data file.	faCardFile	Indicates that the file or directory is in the BasicCard.	faReadOnly	Indicates a read-only file.	faHiddenFile	Indicates a hidden file.	faSystemFile	Indicates a system file.	faArchived	Indicates that file has been backed up since last changed.	faNormal	Indicates that no other attribute bits are set.	faTemporary	Indicates that file is being used for temporary storage.
faDirectory	Indicates that the file is a directory, and not a data file.																
faCardFile	Indicates that the file or directory is in the BasicCard.																
faReadOnly	Indicates a read-only file.																
faHiddenFile	Indicates a hidden file.																
faSystemFile	Indicates a system file.																
faArchived	Indicates that file has been backed up since last changed.																
faNormal	Indicates that no other attribute bits are set.																
faTemporary	Indicates that file is being used for temporary storage.																

These constants are defined in the file FILEIO.DEF.

Access Conditions:

Read access is required to the parent directory (but not to the file itself).

4.4.9 Setting the Current Disk Drive

The **ChDrive** command sets the current disk drive.

ChDrive *drive*

<i>drive</i>	The disk drive for which the current directory is requested. The first character must be a letter ('A-Z' or 'a-z'), or the character '@'.
--------------	---

Note: This command is available in Terminal programs only.

Access Conditions:

No access conditions are required for this command.

4. Files and Directories

Error Codes:

feInvalidDrive The disk drive specified in the *drive* parameter does not exist.

4.4.10 Retrieving the Current Disk Drive

The **CurDrive** function returns the current disk drive as a single-character **String** containing an upper-case letter 'A-Z' or the character '@':

S\$ = CurDrive

Note: This command is available in Terminal programs only.

Access Conditions:

No access conditions are required for this command.

4.5 Creating and Deleting Files

4.5.1 Creating a File

There is no special command to create a new file (but BasicCard files can be defined at compile time – see **4.11 File Definition Sections**). A file is created simply by opening a non-existent file for output, using the **Open** command (see **4.6.1 Opening a File**). A file can't be created in this way if *mode* is **Input** or *access* is **Read**.

4.5.2 Deleting a File

The **Kill** command deletes an existing file:

Kill filename

filename The name of the file.

Access Conditions:

Write access is required, both to the file and to its parent directory.

Error Codes:

feFileNotFound The file does not exist.

feNotDataFile The file is a directory, not a data file. Use **RmDir** to delete directories.

feFileOpen The file can't be deleted, because it is currently open.

4.6 Opening and Closing Files

4.6.1 Opening a File

In traditional Basic, the programmer has to specify *filenum*, the number of the open file slot. But in the BasicCard file system, with open file slots shared between the BasicCard program and the Terminal program, the programmer can't always know which file slots are in use. So ZC-Basic allows an alternative form of the **Open** command, where the operating system automatically selects a free open file slot. (This is equivalent to calling **FreeFile** to select an open file slot, followed by a traditional **Open** command.)

Traditional form: **Open filename [For mode] [Access access] [lock] As [#] filenum [Len=recordlen]**

Alternative form: *filenum* = **Open filename [For mode] [Access access] [lock] [Len=recordlen]**

filename The path name of the file to be opened.

mode If *mode* is **Input**, **Output**, or **Append**, the file is opened for sequential I/O, in which all write operations take place at the end of the file. If *mode* is **Binary** or **Random**, write operations can take place anywhere in the file, overwriting existing data:

Input	Opens the file for sequential input.
Output	Opens the file for sequential output. Existing data is destroyed.
Append	Opens the file for sequential output and sets the file pointer to the end of the file. Existing data in the file is preserved.
Binary	Opens the file for random access by file position, using Get and Put .
Random	Opens the file for random access by record number, using Get and Put .

If the *mode* parameter is absent, its value depends on the *access* parameter: **Input** for **Access Read**, **Output** for **Access Write**, and **Append** for **Access Read Write**. If both *mode* and *access* are absent, *mode* defaults to **Input** and *access* defaults to **Read**.

access Specifies which types of operations will be executed on the file. It takes the value **Read**, **Write**, or **Read Write**.

- If *mode* is **Input**, then *access*, if present, must be **Read**.
- If *mode* is **Output**, then *access*, if present, must be **Write**.
- If *mode* is **Append**, then *access*, if present, must be **Write** or **Read Write**.
- If *mode* is **Binary** or **Random**, then *access* can take any value; it defaults to **Read Write**.

lock For a file in the PC, this parameter specifies whether the file can be opened simultaneously by other processes. For a file in the BasicCard, it specifies whether the file can be opened simultaneously from the Terminal program and the BasicCard program. It also determines whether a file can be opened simultaneously under different open file slots in the same program. The *lock* parameter can take the following values:

Shared	Allows simultaneous read and write operations by other processes.
Lock Read	Prevents simultaneous read operations by other processes.
Lock Write	Prevents simultaneous write operations by other processes.
Lock Read Write	Prevents simultaneous access by other processes (the default).

filenum The number of an open file slot, by which read and write operations will be executed. In the Terminal program, *filenum* must be between 1 and 32 inclusive. In the BasicCard program, *filenum* must be 1 or 2, unless the number of open file slots has been configured with the **#Files** directive (see 3.3.7 Number of Open File Slots).

recordlen Record length or block length.

- If the file is being created, this parameter specifies the size of its data blocks (see 4.2.3 Storage Requirements for more information). If absent (or zero), the data block size for the new file is 32 bytes. If present, it must be ≤ 8191.
- If *access* is **Random**, this parameter specifies the record length of the file. This record length must be between 1 and 254 inclusive.

Access Conditions:

If the file already exists, the access conditions required depend on the *access* parameter: **Read**, **Write**, or **Read Write**. If the file is being created, **Write** access to the parent directory is required, and the **Read** and **Write** access conditions on the new file are the same as those of the parent directory.

Error Codes:

feFileNotFound	The file does not exist, and could not be created, because: <ul style="list-style-type: none"> • the parent directory does not exist; or • <i>mode</i> is Input; or • <i>access</i> is Read.
feNotDataFile	The file is a directory, not a data file.
feFileOpen	(Traditional form only) Open file slot number <i>filenum</i> is already in use.
feTooManyOpenFiles	(Alternative form only) There are no more free open file slots.
feTooManyCardFiles	(Terminal program only) An attempt was made to open a BasicCard file from a Terminal program, but there are no more free open file slots in the BasicCard.

4. Files and Directories

feNameTooLong	(BasicCard file system only) The file can't be created, because its full path name would be longer than 254 characters.
feRecordTooLong	Either <i>access</i> is Random , and <i>recordlen</i> is greater than 254; or the file is being created, and <i>recordlen</i> is greater than 8191.
feBadParameter	Either <i>access</i> is Random , and <i>recordlen</i> is less than 1 (or absent); or the file is being created, and <i>recordlen</i> is less than 0.
feSharingViolation	The file is already open, and the required shared access is not available.

4.6.2 Closing Files

The **Close** command closes one or more files:

Close [[#] *filenum* [, [#] *filenum* , ...]]

Note: If no parameters are supplied, all open files are closed. (But the P-Code interpreter automatically closes all files on program exit.) If the BasicCard program closes all open files in this way, even files that were opened from the Terminal program are closed. In this way, the BasicCard program can always find a free open file slot when it needs one.

4.7 Writing To Files

4.7.1 Writing to Sequential Files

If a file was opened for writing, with a *mode* parameter equal to **Output** or **Append**, it can be written to with a **Print** or **Write** command. All write operations take place at the end of the file.

The **Print** command outputs data to a sequential file in human-readable format. It has the same format as the **Print** command for displaying data on the screen (see **3.21.1 Screen Output**), except for the initial *#filenum* parameter:

Print *#filenum*, [*field* | *separator*] [*field* | *separator*] ...

<i>filenum</i>	The <i>filenum</i> parameter to the Open command by which the file was opened.
<i>field</i>	Any Byte , Integer , Long , Single , or String expression
<i>separator</i>	';' (semi-colon) Leaves the output column unchanged. ' ,' (comma) Advances the output column to the next output field (an output field is 14 characters wide).
	Spc (<i>n</i>) Prints <i>n</i> space characters.
	Tab (<i>n</i>) Advances the output column to position <i>n</i> .

A new-line character is added at the end, unless the last character is a separator. (So you can stay on the same output line by adding a semi-colon at the end of the command.)

Note: Use of this statement in an Enhanced BasicCard program with a parameter of type **Single** will reduce the amount of user-programmable EEPROM available – see **3.23.5 Single-to-String Conversion** for details.

The **Write** command writes data to a sequential file, in a binary format that is specific to ZC-Basic. If a sequence of values is written to a file with **Write** statements, then the same values can subsequently be read from the file using ZC-Basic **Input** statements (see **4.8.1 Reading from Sequential Files**).

Write [#] *filenum*, *expression-list*

<i>filenum</i>	The <i>filenum</i> parameter to the Open command by which the file was opened.
<i>expression-list</i>	A list of expressions separated by commas. Expressions can be of numerical, string, or user-defined type.

Access Conditions:

The file must have been opened with the *access* parameter equal to **Write** or **Read Write**.

Error Codes:

feInvalidMode	The file was not opened with <i>mode</i> equal to Output or Append .
feInvalidAccess	The file was not opened with <i>access</i> equal to Write or Read Write .

4.7.2 Writing to Binary and Random Files

The **Put** command is used to write to files that were opened with *mode* equal to **Binary** or **Random**. The write operation takes place at the current file position, overwriting any existing data at that position. After the **Put** command, the current file position advances to the next character (for **Binary** files) or the next record (for **Random** files):

Put [#] *filenum*, [*pos*], *data*

<i>filenum</i>	The <i>filenum</i> parameter to the Open command by which the file was opened.
<i>pos</i>	A record number for Random files, and a character position for Binary files. If <i>pos</i> is not present (" Put [#] <i>filenum</i> , , <i>data</i> "), the variable is written to the current file position.
<i>data</i>	A variable or array element, or a String expression.

Access Conditions:

The file must have been opened with the *access* parameter equal to **Write** or **Read Write**.

Error Codes:

feInvalidMode	The file was not opened with <i>mode</i> equal to Binary or Random .
feInvalidAccess	The file was not opened with <i>access</i> equal to Write or Read Write .
feSeekError	<i>pos</i> is an invalid file position.

4.8 Reading From Files

4.8.1 Reading from Sequential Files

If a file was opened for reading, with a *mode* parameter equal to **Input** or **Append**, it can be read with a **Line Input** statement, an **Input** function, or an **Input** statement.

Line Input #*filenum*, *X\$* Reads a string from the file, up to the next new-line character or end-of-file, or until 254 characters have been read (the new-line character, if read, is discarded).

X\$ = **Input** (*len*, [#] *filenum*) The **Input** function reads a given number of characters from the file into a string.

Input #*filenum*, *variable-list* The **Input** statement reads a list of variables from a file, expecting them in the format produced by a corresponding **Write** statement (see **4.7.1 Writing to Sequential Files**). This statement can also appear on the right-hand side of an assignment statement:

n = **Input** #*filenum*, *variable-list*

This returns the number of variables in the list that were successfully input.

<i>filenum</i>	The <i>filenum</i> parameter to the Open command by which the file was opened.
<i>X\$</i>	A variable or array element of type String .
<i>len</i>	The number of characters to read.
<i>variable-list</i>	A list of variables or array elements, separated by commas.

Access Conditions:

The file must have been opened with the *access* parameter equal to **Read** or **Read Write**.

4. Files and Directories

Error Codes:

feInvalidMode	The file was not opened with <i>mode</i> equal to Input or Append .
feInvalidAccess	The file was not opened with <i>access</i> equal to Read or Read Write .
feReadError	The end of file was reached before enough bytes were read.

4.8.2 Reading from Binary and Random Files

The **Get** command is used to read from files that were opened with *mode* equal to **Binary** or **Random**. The read operation takes place at the current file position. After the **Get** command, the current file position advances to the next character (for **Binary** files) or the next record (for **Random** files):

Get [#] *filename*, [*pos*], *variable* [, *len*]

<i>filename</i>	The <i>filename</i> parameter to the Open command by which the file was opened.
<i>pos</i>	A record number for Random files, and a character position for Binary files. If <i>pos</i> is not present (e.g. “ Get <i>filename</i> , , <i>variable</i> ”), the read operation takes place at the current file position.
<i>variable</i>	A variable or array element. If this is of type String , it must be followed by the <i>len</i> parameter; otherwise the <i>len</i> parameter must be absent.
<i>len</i>	The number of characters to read, in the case that <i>variable</i> is of type String .

Access Conditions:

The file must have been opened with the *access* parameter equal to **Read** or **Read Write**.

Error Codes:

feInvalidMode	The file was not opened with <i>mode</i> equal to Binary or Random .
feInvalidAccess	The file was not opened with <i>access</i> equal to Read or Read Write .
feSeekError	File position <i>pos</i> does not exist.
feReadError	The end of file was reached before enough bytes were read.

4.9 File Locking and Unlocking

The commands in this section are valid only for files in the Enhanced BasicCard.

4.9.1 Setting Read and Write Access Conditions

The **Read** and **Write** access conditions of a file or directory are changed with the following commands:

Read Lock *filename* [**Key** = *k1* [, *k2*]]

Read Unlock *filename*

Write Lock *filename* [**Key** = *k1* [, *k2*]]

Write Unlock *filename*

Read Write Lock *filename* [**Key** = *k1* [, *k2*]]

Read Write Unlock *filename*

filename The path name of the file or directory.

k1, *k2* The key numbers required to access the file or directory.

- The **Lock** command with no parameters sets the **Read** and/or **Write** access conditions of the specified file or directory to **Forbidden**.
- The **Lock** command with *k1* or *k2* specified sets the **Read** and/or **Write** access conditions of the specified file or directory to **Keyed** – the file can't be read or written from the Terminal program unless DES encryption is currently active.
- The **Unlock** command sets the **Read** and/or **Write** access conditions of the specified file or directory to **Allowed**.

Access Conditions:

Write access is required to the file or directory, and to its parent directory.

Error Codes:

feNotRemoteFile *filename* is not a BasicCard file or directory.

4.9.2 Setting and Unlocking a Custom Lock

If a file or directory has a **Custom** lock, it can't be read or written from a Terminal program unless the BasicCard program explicitly unlocks it. This allows access to a file or directory to be subject to any conditions, such as the presentation of a valid customer PIN number by the Terminal.

To set a **Custom** lock:

Lock *filename*

To unlock a **Custom** lock (BasicCard program only):

Unlock *filename*

Notes:

1. Once a **Custom** lock is set, it can never be permanently removed. A **Custom** lock is for ever.
2. If a **Custom** lock is unlocked, it can only be accessed from the Terminal program until the card is reset. After the card is reset, the BasicCard program must unlock the file or directory again before the Terminal program can access it.

Access Conditions:

For the "**Lock** *filename*" command, **Write** access is required to the file or directory, and to its parent directory. The "**Unlock** *filename*" command is not allowed in a Terminal program, so access conditions are not relevant.

Error Codes:

feNotRemoteFile *filename* is not a BasicCard file or directory.

feTooManyCustomLocks The maximum allowed number of **Custom** locks are already in place. (The implementation of the **Custom** lock mechanism in the Enhanced BasicCard limits the number of locked files to 125.)

4.9.3 Retrieving the Access Conditions on a File or Directory

The access conditions on a file or directory can be obtained with the **Get Lock** command:

Get Lock *filename*, *LockInfo*

filename The path name of the file or directory.

LockInfo A variable of user-defined type or a fixed-length string, at least seven bytes long. A suitable user-defined type **LockInfo** is defined in FILEIO.DEF:

```

Type LockInfo
  ReadLock As Byte
  WriteLock As Byte
  CustomLock As Byte
  ReadKey1@, ReadKey2@
  WriteKey1@, WriteKey2@
End Type

```

ReadLock and **WriteLock** can be **liAllowed**, **liForbidden**, **liKeyed1**, or **liKeyed2**. If **liKeyed1** or **liKeyed2**, then **ReadKey1@** etc. contain the appropriate key numbers.

CustomLock can be **liAllowed**, **liUnlocked**, or **liLocked**.

Access Conditions:

Read access is required to the parent directory.

Error Codes:

feNotRemoteFile *filename* is not a BasicCard file or directory.

4. Files and Directories

Note: Enhanced BasicCard versions ZC3.3, ZC3.4, ZC3.5, and ZC3.6 contains a bug in the file access code that can result in access being denied when it should be granted. This bug only occurs when a file has a lock of type **liKeyed1**. To get round this bug, the compiler automatically converts all such locks to type **liKeyed2**, with a dummy key number 255 as the second key.

4.10 Miscellaneous File Operations

<i>filenum</i> = FreeFile	Returns a free <i>filenum</i> for use in a traditional Open statement. Returns -1 if no more file numbers are available, with error code feTooManyOpenFiles .
Seek [#] <i>filenum</i> , <i>pos</i>	Sets the file pointer to position <i>pos</i> (of type Long) for the next read or write operation on file <i>filenum</i> . <i>pos</i> is a record number for files opened with <i>mode</i> = Random ; otherwise it is a byte count. Records and bytes are numbered from 1. <i>Note:</i> If the file contains less than <i>pos</i> -1 bytes (or records), Seek fails with error code feSeekError , unless the file was opened for output in random access mode (<i>mode</i> = Binary or <i>mode</i> = Random , with Write access specified). In this case, the file is filled with zeroes to the required length.
Seek ([#] <i>filenum</i>)	Returns the read/write position for file <i>filenum</i> , as a Long value.
Len (# <i>filenum</i>)	Returns the length of file <i>filenum</i> in bytes, as a Long value.
EOF ([#] <i>filenum</i>)	Returns True if the end of file has been reached.

4.11 File Definition Sections

Using File Definition Sections, files and directories can be defined in the source code of the BasicCard program, to be created by the compiler. Files and directories so defined are downloaded to the BasicCard together with the BasicCard program itself. A File Definition Section begins with a **Dir** command and ends with the matching **End Dir** command. It may occur anywhere in an Enhanced BasicCard program; it may contain only File Definition statements, not regular ZC-Basic statements. A program may contain any number of File Definition Sections.

4.11.1 Directory Definition

Dir *path*

Lock Definitions

File Definitions

Sub-directory Definitions

End Dir

<i>path</i>	The path name of the directory. It may be a new directory or an existing directory.
<i>Lock Definitions</i>	Lock and Unlock statements for the <i>path</i> directory. These have the same format as the statements described in 4.9 File Locking and Unlocking , but without the <i>filename</i> parameter.
<i>File Definitions</i>	Definitions of files contained in the <i>path</i> directory (see 4.11.2 File Definition).
<i>Sub-directory Definitions</i>	Nested Directory Definitions, defining sub-directories of the <i>path</i> directory. Each nested Directory Definition must end with its own End Dir statement.

File Definitions and nested Directory Definitions may occur in any order.

4.11.2 File Definition

A File Definition may occur only inside a Directory Definition. It ends with the next **File** or **Dir** statement, or with the **End Dir** statement of the enclosing Directory Definition.

File *filename* [**Len** = *blocklen*]

Lock Definitions

Data Definitions

filename The path name of the file.

blocklen The size of the new file's data blocks (see **4.2.3 Storage Requirements** for more information). If absent, *blocklen* defaults to 32.

Lock Definitions **Lock** and **Unlock** statements for the file. These have the same format as the statements described in **4.9 File Locking and Unlocking**, but without the *filename* parameter.

Data Definitions The initial data contained in the file. A Data Definition statement looks like this:

expr [**As** *type*] [(*repeat-count*)] [, *expr* [**As** *type*] [(*repeat-count*)], ...]

expr Any constant expression of numerical or string type.

type A data type. If absent, it defaults to the smallest data type that can contain *expr*. If *type* is a fixed-length string longer than *expr*, it is padded with NULL characters (ASCII zeroes) to the required length.

(*repeat-count*) The number of copies of *expr* to store in the file.

Note: To store a new-line character in the data, use the constant 10.

4.12 The Definition File FILEIO.DEF

```
Rem  FILEIO.DEF
Rem
Rem  Declarations for ZC-Basic File I/O

#IfNotDef FileioDefIncluded ' Prevent multiple inclusion
Const FileioDefIncluded = True

#IfDef CompactBasicCard
#Error File I/O is not supported in the Compact BasicCard!
#EndIf

Rem  FileError codes

Const feFileOK                = 0
Const feInvalidDrive          = 1
Const feBadFilename           = 2
Const feBadFilenum            = 3
Const feFileNotFound          = 4
Const feFileNotOpen           = 5
Const feOpenError             = 6
Const feSeekError             = 7
Const feReadError             = 8
Const feWriteError            = 9
Const feCloseError            = 10
Const feInvalidMode           = 11
Const feInvalidAccess         = 12
Const feRenameError           = 13
Const feAccessDenied          = 14
Const feSharingViolation      = 15
```


4. Files and Directories

```
Const feFileAlreadyExists    = 16
Const feNotDataFile          = 17
Const feNotDirectory         = 18
Const feDirNotEmpty          = 19
Const feBadFileChain         = 20
Const feFileOpen             = 21
Const feNameTooLong          = 22
Const feRecordTooLong        = 23
Const feTooManyOpenFiles     = 24
Const feTooManyCardFiles     = 25
Const feCommsError           = 26
Const feRemoteFile           = 27
Const feNotRemoteFile        = 28
Const feRecursiveRename      = 29
Const feInvalidFromKeyboard  = 30
Const feBadParameter         = 31
Const feOutOfMemory          = 32
Const feNoFileSystem         = 33
Const feUnexpectedError      = 34
Const feNotImplemented       = 35
Const feTooManyCustomLocks   = 36
Const feBadKeyFile           = 37
```

Rem File Attribute bits

```
Const faDirectory = &H0010
Const faCardFile  = &H0040
```

#IfDef TerminalProgram

```
Const faReadOnly    = &H0001
Const faHiddenFile  = &H0002
Const faSystemFile  = &H0004
Const faArchived    = &H0020
Const faNormal       = &H0080
Const faTemporary   = &H0100
```

#EndIf

Rem LockInfo defined type, for GET LOCK statement

Type LockInfo

```
ReadLock As Byte      ' liAllowed, liKeyed1, liKeyed2, or liForbidden
WriteLock As Byte     ' liAllowed, liKeyed1, liKeyed2, or liForbidden
CustomLock As Byte    ' liAllowed, liUnlocked, or liLocked
ReadKey1@, ReadKey2@  ' Key number(s) for ReadLock
WriteKey1@, WriteKey2@ ' Key number(s) for WriteLock
```

End Type

Rem LockInfo constants

```
Const liAllowed      = 0
Const liKeyed1       = 1
Const liKeyed2       = 2
Const liForbidden    = 3
Const liUnlocked     = 1
Const liLocked       = 2
```

#EndIf ' FileioDefIncluded

5. Support Software

This document describes Version 4.50 of the ZeitControl MultiDebugger software support package. All the software described in this chapter is available free of charge from our web site at www.BasicCard.com.

5.1 Hardware Requirements

No special hardware is required to develop programs in ZC-Basic – the support software can simulate the BasicCard inside your PC, so you can compile and test software on any Windows® 98/NT/2000 system.

Once the software is written and tested, you will need a PC/SC-compatible card reader, and one or more BasicCards. ZeitControl offers a selection of card readers – see our web site for details. A development kit containing CyberMouse reader, BasicCards, and printed documentation is available from ZeitControl – contact us at Sales@ZeitControl.de.

5.2 Installation

Please obtain the latest version of our development software before installing it. The latest version is available free of charge from our web site at www.BasicCard.com. Installation instructions can be found there.

To install the BasicCard software from the CD, run the program BasicPro\Setup.exe. The software is installed in the directory C:\BasicCardPro unless you specify a different destination.

5.3 File Types

To use the development software effectively, it helps to have a clear idea of the roles played by the different types of files used by the system. We can arrange the files in a three-level hierarchy: *Project Files*, *Program Files*, and *Source Files*. There is a corresponding software hierarchy: development environment **ZCPDE**; debuggers **ZCMDTERM/ZCMDCARD**; and compiler **ZCMBASIC**:

Level 1: Project Files



*.**ZCP** Project Files

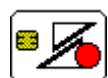
ZCPDE.EXE ZeitControl Professional Development Environment

Level 2: Program Files



*.**ZCT** Terminal Program Files

ZCMDTERM.EXE ZeitControl Terminal Program Debugger



*.**ZCC** BasicCard Program Files

ZCMDCARD.EXE ZeitControl BasicCard Program Debugger

Level 3: Source Files



*.**BAS** ZC-Basic Source Files

*.**DEF** ZC-Basic Definition Files

ZCMBASIC.EXE ZeitControl ZC-Basic Compiler

5. Support Software

This hierarchy is not strictly enforced – you can run the debuggers outside the development environment if you just want to test a simple program; or you can compile a program from the Win32 console command line if you don't need to debug it.

**.ZCP Project Files*

A Project File simply lists all the Program Files that belong to a single project. What constitutes a project is up to you; the simplest projects contain one Terminal Program File and one BasicCard Program File, but bigger projects may contain two or three Terminal Program Files and a dozen or so BasicCard Program Files.

**.ZCT Terminal Program Files*

A Terminal Program File contains:

- compiler options for a Terminal Program, including Source File, Include Paths, and Pre-Defined Constants;
- run-time options, such as initial COM Port and Terminal Program command-line parameters;
- the positions of the various windows.

**.ZCC BasicCard Program Files*

A BasicCard Program File can be thought of as a Virtual BasicCard. It contains:

- compiler options for a BasicCard Program, including Source File, Card Type, Include Paths, and Pre-Defined Constants;
- the EEPROM contents of the Virtual BasicCard;
- the COM Port of the Virtual Card Reader that the program occupies;
- the positions of the various windows.

You can have more than one BasicCard Program File for a given source program, each with its own Virtual EEPROM. And you can run more than one **ZCMD CARD** BasicCard Debugger at a time, as long as no two debuggers occupy the same Virtual Card Reader COM Port.

**.BAS and *.DEF ZC-Basic Source Files*

In our example programs, we make the distinction between .BAS files, which contain code, and .DEF files, which contain only definitions and declarations. This distinction is purely conventional; the compiler doesn't treat the two file types differently.

ZC-Basic Source Files are fully described in **3The ZC-Basic Language**.

In addition, the **ZCMBASIC** Compiler produces the following two file types as output (among others – see **5.9.1 The ZC-Basic Compiler ZCMBASIC.EXE** for details):

**.IMG Image Files*

An Image File contains a compiled Terminal Program or BasicCard Program, with no symbolic debug information. Its contents are described in **10.1 ZeitControl Image File Format**. Two command-line programs accept Image Files as input (and Debug Files too, if the .DBG file extension is explicitly given):

- the **ZCMSIM** P-Code Interpreter, which requires a Terminal Program Image File, and optionally one or more BasicCard Program Image Files;
- the **BCLOAD** Download Program, which downloads a BasicCard Image File to a BasicCard.

See **5.9.2 The P-Code Interpreter ZCMSIM.EXE** and **5.9.3 The Card Loader BCLOAD.EXE** for details.

**.DBG Debug Files*

A Debug File contains all the information in an Image File, plus symbolic debug information for the debuggers **ZCMDTERM** and **ZCMD CARD**. Its contents are described in **10.2 ZeitControl Debug File Format**.

5.4 Physical and Virtual Card Readers

Whenever you access a BasicCard or a Card Reader from a ZC-Basic Terminal Program, ZeitControl's P-Code Interpreter uses the current value of the **ComPort** variable to determine where to look for the Card Reader. The meaning of the **ComPort** variable depends on the program that contains the P-Code Interpreter: this can be an executable file, the **ZCMSIM** P-Code Interpreter, or the **ZCMDTERM** Terminal Program Debugger.

5.4.1 ComPort in an Executable File

A ZC-Basic program compiled into an executable file accepts the following values for the **ComPort** variable:

- 1 <= **ComPort** <= 4: Physical Card Reader on serial port COM1-COM4
- 100 <= **ComPort** <= 199: PC/SC Card Reader – see **3.21.4 PC/SC Functions**
- 201 <= **ComPort** <= 204: Virtual Card Reader running in the **ZCMDCARD** debugger

5.4.2 ComPort in the ZCMSIM P-Code Interpreter

The **ZCMSIM** P-Code Interpreter accepts the same values for the **ComPort** variable as an executable file, as listed in the previous section. In addition, **ComPort** may be set to any of the **-P** parameters specified on the command line, in which case the corresponding simulated BasicCard is accessed – see **5.9.2 The P-Code Interpreter ZCMSIM.EXE**.

5.4.3 ComPort in the ZCMDTERM Terminal Program Debugger

The **ZCMDTERM** Terminal Program Debugger accepts the following values for the **ComPort** variable:

- 1 <= **ComPort** <= 4: Physical or Virtual Card Reader
- 100 <= **ComPort** <= 199: PC/SC Card Reader – see **3.21.4 PC/SC Functions**
- 201 <= **ComPort** <= 204: Virtual Card Reader running in the **ZCMDCARD** debugger

If 1 <= **ComPort** <= 4, then **ZCMDTERM** has to decide whether to access a Physical or a Virtual Card Reader. It does this on the basis of the settings in the **Options|Terminal Programs...|Card Readers** dialog box. In this dialog box, each of COM1 through COM4 can be set to **Real**, **Auto**, or **Virtual**:

- Real** Physical Card Reader is accessed
- Auto** Virtual Card Reader if available, otherwise Physical Card Reader
- Virtual** Virtual Card Reader running in the **ZCMDCARD** debugger

To enable communication between the Terminal Program and a BasicCard program running in the **ZCMDCARD** BasicCard Program debugger, the **ZCMDCARD** debugger must know which COM Port to attach to. You can specify this in one of two ways:

- in **ZCMDCARD**, via the **Card|Insert in Virtual Reader...** dialog box;
- in **ZCMDCARD** or **ZCPDE**, via the **Options|BasicCard Program...|COM Ports** dialog box.

The first of these is temporary; the second is permanent for the given BasicCard Program File.

5.5 Windows-Based Software

The Windows-based software consists of the following programs:

- **ZCPDE**, the ZeitControl Professional Development Environment. This program manages projects, creating and maintaining ZeitControl Project files, with **.ZCP** extension. It also contains a built-in text editor.
- **ZCMDTERM**, a source-level symbolic debugger for Terminal programs. It can communicate with one or more **ZCMDCARD** debuggers, and one or more physical card readers. It uses ZeitControl Terminal Program files, with **.ZCT** extension, to store the information that it needs to compile and run Terminal Programs.

5. Support Software

- **ZCMDCARD**, a source-level symbolic debugger for BasicCard programs. It waits for commands from the Terminal debugger **ZCMDTERM**, executes the commands under the control of the user, and sends its responses back to the Terminal debugger. It can also download BasicCard programs to a real BasicCard. It uses ZeitControl BasicCard Program files, with **.ZCC** extension, to store the information that it needs to compile and run BasicCard Programs.

5.6 The ZCPDE Professional Development Environment



The **ZCPDE** ZeitControl Professional Development Environment program manages projects, creating and maintaining ZeitControl Project files, with **.ZCP** extension. It also contains a built-in text editor.

5.6.1 ZCPDE File Menu

The File menu is for editing text files, and contains no project management functions. It contains the following items:

New	Create a new text file
Open...	Open an existing text file
Reopen ►	Open a recently opened text file
Save	Save the current text file
Save As...	Save the current text file under a new name
Save All	Save all modified files
Close	Close the current text file
Print...	Print the current text file
Printer Setup...	Set printer options
Exit	Exit the ZCPDE program

5.6.2 ZCPDE Edit Menu

The Edit menu is for editing text files, and contains no project management functions. It contains the following items:

Undo	Undo the most recent edit operation
Redo	Redo an operation that was cancelled with Undo
Cut	Delete text and place it in the clipboard
Copy	Copy text to the clipboard
Paste	Copy text from the clipboard
Delete	Delete text without placing it in the clipboard
Select All	Select the whole text file
Find...	Search for text
Find Next	Find the next occurrence of the most recent search text
Replace...	Search and replace

5.6.3 ZCPDE Project Menu

This menu contains the project management functions:

New	Create a new project						
Open...	Open an existing project						
Reopen ►	Open a recently opened project						
Save As...	Save the current project under a different name						
Options	Set the Project Options: <table border="0" data-bbox="662 1691 1331 1787"> <tr> <td><i>Terminal Programs</i></td><td>The project's Terminal Program Files</td></tr> <tr> <td><i>BasicCard Programs</i></td><td>The project's BasicCard Program Files</td></tr> <tr> <td><i>Start Configuration</i></td><td>The programs run by the Start item</td></tr> </table>	<i>Terminal Programs</i>	The project's Terminal Program Files	<i>BasicCard Programs</i>	The project's BasicCard Program Files	<i>Start Configuration</i>	The programs run by the Start item
<i>Terminal Programs</i>	The project's Terminal Program Files						
<i>BasicCard Programs</i>	The project's BasicCard Program Files						
<i>Start Configuration</i>	The programs run by the Start item						
Start Terminal ►	Start a Terminal Program in the ZCMDTERM debugger						
Start BasicCard ►	Start a BasicCard Program in the ZCMDCARD debugger						
Start	Start all programs in the current project's Start Configuration						
Compile Terminal ►	Compile a Terminal Program from the current project						
Compile BasicCard ►	Compile a BasicCard Program from the current project						
Compile Again	Re-compile the most recently compiled program						
Compile All	Compile all the programs in the current project						

5. Support Software

5.6.4 ZCPDE Options Menu

This menu sets the global options for the **ZCPDE** program. It contains a single item, which brings up a multi-page dialog box:

Environment	<i>Editor</i>	Set tab width and font
	<i>Compiler</i>	Set Include Path, in Windows Registry variable “ Software\ZeitControl\BasicCardPro\ZCINC ”
	<i>CardReader</i>	Set default ComPort , in Windows Registry variable “ Software\ZeitControl\BasicCardPro\ZCPORT ”

5.6.5 ZCPDE Help Menu

This menu contains the following items:

BasicCard Manual	Open this manual on-line
Open Example ▶	Open one of the BasicCard example projects
About...	Display software version number and product information

5.7 The ZCMDTERM Terminal Program Debugger



The **ZCMDTERM** ZeitControl Terminal Program Debugger is a source-level symbolic debugger for Terminal programs. It can communicate with one or more **ZCMDCARD** debuggers, and one or more physical card readers. It uses ZeitControl Terminal Program files, with **.ZCT** extension, to store the information that it needs to compile and run Terminal Programs.

5.7.1 ZCMDTERM File Menu

The File menu contains the following items:

New	Create a new Terminal Program File
Open...	Open an existing Terminal Program File
Save	Save the current Terminal Program File
Save As...	Save the current Terminal Program File under a new name
Edit...	Edit a text file in the ZCPDE Professional Development Environment
Edit Source ▶	Edit a source file from the current Terminal Program
Compile...	Short cut to the Options Terminal Program... Compiler dialog box
Exit	Exit the ZCMDTERM program

5.7.2 ZCMDTERM View Menu

The View menu contains the following items:

Source File ▶	Display a selected source file in the debugger window
Procedure ▶	Display a selected ZC-Basic procedure in the debugger window
P-Code	Display P-Code instructions and registers in the debugger window
Watches	Open the Watches window for monitoring program data
I/O	Open the I/O window for monitoring I/O between Terminal and BasicCard

5.7.3 ZCMDTERM Run Menu

The Run menu contains the following items:

Run	Start execution from the current PC
Step Over	Execute one instruction, stepping over procedure calls
Step Into	Execute one instruction, stepping into procedure calls
Step Return	Execute until the end of the current procedure
Step to Card	Run until an instruction in a BasicCard program is reached
Step to Cursor	Run to the current cursor position
Restart	Restart the Terminal Program
Pause	Interrupt execution
Evaluate...	Evaluate an expression

Most of these items are also available as short-cut buttons in the debugger window, unless the **Options|Hide Buttons** menu item was selected.

5.7.4 ZCMDTERM Options Menu

Terminal Program...	Set the Terminal Program options:
	<i>Compiler</i> Source file, include paths, etc.
	<i>Run-time</i> COM port, log file, command-line parameters
	<i>Card Readers</i> See 5.4.3 ComPort in the ZCMDTERM Terminal Program Debugger
COM Port...	Short cut to Terminal Program... Run-time dialog box
Show/Hide Buttons	Show or hide the Run menu short-cut buttons

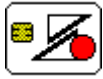
5. Support Software

5.7.5 ZCMDTERM Help Menu

This menu contains the following items:

BasicCard Manual	Open this manual on-line
About...	Display software version number and product information

5.8 The ZCMDCARD BasicCard Program Debugger



The **ZCMDCARD** ZeitControl BasicCard Program Debugger is a source-level symbolic debugger for BasicCard programs. It waits for commands from the Terminal debugger **ZCMDTERM**, executes the commands under the control of the user, and sends its responses back to the Terminal debugger. It can also download BasicCard programs to a real BasicCard. It uses ZeitControl BasicCard Program files, with **.ZCC** extension, to store the information that it needs to compile and run BasicCard Programs.

5.8.1 ZCMDCARD File Menu

The File menu contains the following items:

New	Create a new BasicCard Program File
Open...	Open an existing BasicCard Program File
Save	Save the current BasicCard Program File
Save As...	Save the current BasicCard Program File under a new name
Edit...	Edit a text file in the ZCPDE Professional Development Environment
Edit Source ▶	Edit a source file from the current BasicCard Program
Compile...	Short cut to the Options BasicCard Program... Compiler dialog box
Exit	Exit the ZCMDCARD program

5.8.2 ZCMDCARD View Menu

The View menu contains the following items:

Source File ▶	Display a selected source file in the debugger window
Procedure ▶	Display a selected ZC-Basic procedure in the debugger window
P-Code	Display P-Code instructions and registers in the debugger window
Watches	Open the Watches window for monitoring program data
I/O	Open the I/O window for monitoring I/O between Terminal and BasicCard
File System	View files and directories in the BasicCard

5.8.3 ZCMDCARD Run Menu

The Run menu contains the following items:

Run	Start execution from the current PC
Step Over	Execute one instruction, stepping over procedure calls
Step Into	Execute one instruction, stepping into procedure calls
Step Return	Execute until the end of the current procedure
Step to Terminal	Run until an instruction in the Terminal program is reached
Step to Cursor	Run to the current cursor position
Pause	Interrupt execution
Evaluate...	Evaluate an expression

Most of these items are also available as short-cut buttons in the debugger window, unless the **Options|Hide Buttons** menu item was selected.

5.8.4 ZCMDCARD Card Menu

Insert in Virtual Reader ▶	Attach ZCMDCARD to a Virtual Card Reader COM Port
Remove from Virtual Reader	Release the Virtual Card Reader COM Port
Download to Real Card...	Download the BasicCard program to a real BasicCard

5. Support Software

5.8.5 ZCMDCARD Options Menu

BasicCard Program...	Set the BasicCard Program options:
	<i>Compiler</i> Source file, card type, include paths, etc.
	<i>COM Ports</i> Virtual and Physical Card Reader COM Ports
Show/Hide Buttons	Show or hide the Run menu short-cut buttons

5.8.6 ZCMDCARD Help Menu

This menu contains the following items:

BasicCard Manual	Open this manual on-line
About...	Display software version number and product information

5.9 Command-Line Software

The following programs are run from a Win32 command-line console (or “DOS box”):

- **ZCMBASIC**, a compiler for the ZC-Basic programming language.
- **ZCMSIM**, a P-Code interpreter that runs compiled ZC-Basic programs. **ZCMSIM** runs a Terminal program, and can run BasicCard programs simultaneously in simulated BasicCards, or communicate via a card reader with genuine BasicCards.
- **BCLOAD**, for downloading P-Code to the BasicCard.
- **KEYGEN**, a program that generates random keys and primitive polynomials for use in encryption.
- **BCKEYS**, for downloading keys to the Compact and Enhanced BasicCards.

Each of these programs takes a filename as its main parameter. Other command-line parameters begin with ‘-’ (minus sign) followed by one or more option letters, sometimes followed by data. No spaces are allowed between the minus sign and the option letters, or between the option letters and the data. Option letters may be upper or lower case.

ZCMBASIC, **ZCMSIM**, and **BCLOAD** support parameter input files: if any command-line parameter has the form ‘@filename’, subsequent parameters are read from the given file, one line at a time. Empty lines, and lines whose first non-space character is a single quote, are ignored. To specify a parameter that begins with the ‘@’ character, simply repeat the ‘@’ character; for example, “@@X” is passed to the program as “@X”, and is not treated as a parameter file. This feature is also active for executable files created by the **ZCMBASIC** compiler.

Notes:

- Three of these programs – **ZCMSIM**, **BCLOAD**, and **BCKEYS** – communicate with a card reader, via a serial port or the PC/SC driver. The default value of the COM port is taken from the environment variable **ZCPORT**; or the Windows Registry variable “HKEY_CURRENT_USER\Software\ZeitControl\BasicCardPro\ZCINC” if this environment variable does not exist; or 1 if neither of these variables exists. (To specify PC/SC reader number *n*, set the COM port to 100+*n*.)
- If a filename parameter contains spaces, it must be enclosed in quotation marks on the command line. (For example: **ZCMBASIC -OI "Hello World"** compiles the file “**Hello World.BAS**” and creates the file “**Hello World.IMG**”.)

5. Support Software

5.9.1 The ZC-Basic Compiler ZCMBASIC.EXE

The compiler **ZCMBASIC.EXE** takes ZC-Basic source code as input, and produces P-Code as output. It compiles the entire program in one pass; there is no linking stage. To run the compiler:

ZCMBASIC [*param* [*param* ...]] *input-file* [*param* [*param* ...]]

input-file The ZC-Basic source file. If no file extension is supplied, *input-file.bas* is assumed.

param One of the following:

- Ctype** Compiles code for the given virtual machine type:
 - CT** or **-C0** Terminal (the default).
 - CC1** or **-C1.1** Compact BasicCard version **ZC1.1**
 - CEn** or **-C3.n** Series 3 Enhanced BasicCard version **ZC3.n**
 - CFfilename** Professional BasicCard with Configuration File *filename*.
If no file extension is supplied, *filename.zcf* is assumed.

See Sections 1.6–1.8 for information about the different BasicCard types.

- Dsymbol[=val]** Defines *symbol* as if the source program contained the statement **Const symbol=val**. The *val* parameter must be an integer or a string; arithmetic expressions are not allowed. If *val* is absent, it defaults to 1.
- E[exe-file]** Creates an executable file that will run in a DOS box under Windows® 98. If no file extension is supplied, *exe-file.exe* is created. If *exe-file* is absent, *input-file.exe* is created.

- Ipath** Adds *path* to the list of directories to search for **#Include** files (see 3.3.1 **Source File Inclusion**). A closing backslash in *path* is optional. Multiple paths may be supplied, separated by semicolons.

- OI[image-file]** Generates an image file. If no file extension is supplied, *image-file.img* is created. If *image-file* is absent, *input-file.img* is created.

The image file is described in 10.1 **ZeitControl Image File Format**.

- OD[debug-file]** Generates a debug information file. If no file extension is supplied, *debug-file.dbg* is created. If *debug-file* is absent, *input-file.dbg* is created.

The debug file is described in 10.2 **ZeitControl Debug File Format**.

- OL[list-file]** Generates a list file. If no file extension is supplied, *list-file.lst* is created. If *list-file* is absent, *input-file.lst* is created.

The list file is described in 10.3 **List File Format**.

- OM[map-file]** Generates a map file. If no file extension is supplied, *map-file.map* is created. If *map-file* is absent, *input-file.map* is created.

The map file is described in 10.4 **Map File Format**.

- OE[error-file]** Writes all error messages to a file. If *error-file* already exists, it is deleted before compilation begins. If no file extension is supplied, *error-file.err* is created. If *error-file* is absent, *input-file.err* is created.

- Sstack-size** Sets the size of the P-Code stack. Normally the compiler can work out for itself how big the stack has to be. But if the program contains recursive procedure calls or recursive **GoSub** calls, the compiler must guess the stack size, because it can't know how deep the recursion will go. You can override this guess with **-Sstack-size** (or with the **#Stack** pre-processor directive – see 3.3.8 **Stack Size**).

- Sstate** Switches the card into the specified state after the P-Code is downloaded. See also 3.3.6 **Card State**. Only the first letter of *state* is significant:

First letter of <i>state</i> :	'L'	'P'	'T'	'R'
New card state:	LOAD	PERS	TEST	RUN

5.9.2 The P-Code Interpreter ZCMSIM.EXE

The program **ZCMSIM.EXE** loads and runs a compiled ZC-Basic Terminal program from a ZeitControl Image File (or Debug File). It can also simultaneously run one or more BasicCard programs in simulated BasicCards, or it can communicate with real BasicCards via physical card readers. To run the **ZCMSIM** program:

ZCMSIM [*param* [*param* . . .]] *image-file* [*P1*\$ [*P2*\$. . .]]

Parameters *before* the image-file name are processed by the **ZCMSIM** program, as described below. Parameters *after* the image-file name (*P1*\$, *P2*\$,...) are passed to the Terminal program via the pre-defined **String** array **Param\$(1 To nParams)** – see **3.21.10 Pre-Defined Variables**.

image-file The image file output by the compiler. If no file extension is supplied, *image-file.img* is assumed. (So if this is a Debug File, the **.dbg** extension must be present.)

param One of the following:

- Ccard-file** The image file of a BasicCard program. If this parameter is present, **ZCMSIM** simulates a BasicCard in the PC.
- L[log-file]** Generates a log file, containing the commands sent to the card and their responses. If no file extension is supplied, *log-file.log* is created. If *log-file* is absent, *image-file.log* is created.
- Pcom-port** The number of the COM port that the card reader is attached to. (This can also be set from within the Terminal program itself, via the **ComPort** pre-defined variable.) This parameter may appear more than once – see *Note* below.
- W** Write the EEPROM data back to the image file(s) when the Terminal program exits. The Terminal program EEPROM data is written back to *image-file*. If the **-C** parameter is present on the command line, the EEPROM data in the simulated BasicCard program is written back to *card-file* when the Terminal program exits.
- WT[new-file]** Write the Terminal program EEPROM data back to *new-file* when the Terminal program exits. If no file extension is supplied, *new-file.img* is created. If *new-file* is absent, the EEPROM data is written back to *image-file*.
- WC[new-file]** Write the EEPROM data in the simulated BasicCard program back to *new-file* when the Terminal program exits. If no file extension is supplied, *new-file.img* is created. If *new-file* is absent, the EEPROM data is written back to *card-file*.

P1\$, *P2*\$,... These parameters are separated by spaces or tabs. To pass a space or tab in a parameter, enclose it in quotation marks; to pass a quotation mark in a parameter, precede it with a backslash. (Backslashes not followed by quotation marks are passed as is.)

Note: If multiple **-P** parameters are present:

- **-C** and **-WC** apply to the card on the most recently specified COM port;
- the **ComPort** variable is set from the last **-P** parameter.

For instance, to communicate with a simulated BasicCard program on COM1 and a real BasicCard on COM2:

ZCMSIM -P1 -Ccard-file -P2 image-file

5. Support Software

5.9.3 The Card Loader BCLOAD.EXE

The program **BCLOAD.EXE** downloads P-Code and data to the BasicCard.

The ZC-Basic compiler produces a ZeitControl Image File as output, containing P-Code and data in binary form. To run the **BCLOAD** program:

BCLOAD [*param* [*param* . . .]] *image-file* [*param* [*param* . . .]]

image-file The image file output by the compiler. If no file extension is supplied, *image-file.img* is assumed. (A debug file is also allowed here; in this case, the **.dbg** extension must be supplied.)

param One of the following:

- D** Displays the commands on the screen as they are executed.
- L[*log-file*]** Generates a log file, containing the commands sent to the card and their responses. If no file extension is supplied, *log-file.log* is created. If *log-file* is absent, *image-file.log* is created.
- E[*error-file*]** Writes all error messages to a file. If *error-file* already exists, it is deleted before the download begins. (So if *error-file* exists after the program exits, it means that an error occurred.) If no file extension is supplied, *error-file.err* is created. If *error-file* is absent, *image-file.err* is created.
- P*com-port*** The number of the COM port that the card reader is attached to.
- S*state*** Switches the card into the specified state after the download. Only the first letter of *state* is significant:

First letter of <i>state</i> :	'L'	'P'	'T'	'R'
New card state:	LOAD	PERS	TEST	RUN

Note: The ZC-Basic source code for this program is supplied on the distribution disk, in the BasicCardPro\Source\BCLoad directory. **BCLOAD.EXE** was compiled with the COMPILE.BAT command file in the same directory.

5.9.4 The Key Generator *KEYGEN.EXE*

The program **KEYGEN.EXE** generates cryptographic keys and primitive polynomials for the encryption and decryption of commands and responses. It creates a ZC-basic source file containing **Declare Key** and/or **Declare Polynomial** statements. This file can be **#Included** in the source code of the Terminal and BasicCard programs, or it can be downloaded separately to a Compact or Enhanced BasicCard using the **BCKEYS** Key Loader program. The program prompts the user to press keys on the keyboard at random; the cryptographic keys and polynomials are generated from this user input, after hashing with the **MD5** algorithm (see R.L. Rivest, “The MD5 Message Digest Algorithm”, RSA Data Security, Inc., April 1992). To run the **KEYGEN** program:

```
KEYGEN [ param [ param ... ] ] key-file [ param [ param ... ] ]
```

key-file The name of the key file to create or update. If no file extension is supplied, *key-file.bas* is assumed.

param One of the following:

-K*key*[(*len*[, *count*])] *key* is a key number between 0 and 255; *len* is a key length between 1 and 255; and *count* is the initial value of the error counter for the key, between 0 and 15 (see **3.17.2 Key Declaration**). If *len* is absent, it defaults to 8; if *count* is absent, the error counter for the key is disabled. You can create multiple keys by specifying the **-K** parameter more than once.

-P Generates two random primitive polynomials for use by the **SG-LFSR** encryption algorithms.

-Q Generates random numbers quickly, without requiring keyboard input from the user.

Note: This feature is provided for convenience of use during the development of an application. Keys and polynomials generated with the **-Q** parameter should not be used in a released application, as this might compromise the security of the encryption algorithms.

-U *key-file* is updated, rather than being created from scratch – existing keys and polynomials in *key-file* are preserved, unless overridden by **-K** or **-P**.

Note: The generation of cryptographic keys is a delicate business. The security of the encryption algorithms used by the BasicCard relies on the secrecy of the keys and polynomials generated by the **KEYGEN** program, which in turn relies on the quality of the random number generator. To foster confidence in the security of our product, we provide the C++ source code of the **KEYGEN** program in the directory BasicCardPro\Source\Keygen.

5. Support Software

5.9.5 The Key Loader BCKEYS.EXE

The program **BCKEYS.EXE** downloads cryptographic keys and/or polynomials to a Compact or Enhanced BasicCard. The following conditions apply to the downloading of keys and polynomials:

- The BasicCard must be in state **LOAD** (or switchable to state **LOAD**);
- The BasicCard must already have been loaded with P-Code and data by the **BCLOAD** program;
- All keys that you want to download must have been declared in the ZC-Basic source code, with **Declare Key** statements.

The program takes a key file as input. This is a ZC-Basic source file that contains only **Declare Key** and/or **Declare Polynomials** statements. The **KEYGEN** program can generate key files for you – see **5.9.4 The Key Generator KEYGEN.EXE**.

To run the **BCKEYS** program:

BCKEYS [*param* [*param* . . .]] *key-file* [*param* [*param* . . .]]

key-file The key file, as described above. If no file extension is supplied, *key-file.bas* is assumed.

param One of the following:

- K**[*key*] *key* is a key number between 0 and 255. You can download multiple keys by specifying this parameter more than once. If *key* is absent, all the keys in *key-file* are downloaded.
- P** Downloads the polynomials to the BasicCard.

If neither –**K** nor –**P** appears on the command line, then all the keys and polynomials in *key-file* are downloaded.
- L**[*log-file*] Generates a log file, containing the commands sent to the card and their responses. If no file extension is supplied, *log-file.log* is created. If *log-file* is absent, *key-file.log* is created.
- D** Displays the commands on the screen as they are executed.
- P***com-port* The number of the COM port that the card reader is attached to.
- S***state* Switches the card into the specified state after the download. Only the first letter of *state* is significant:

First letter of <i>state</i> :	‘L’	‘T’	‘R’
New card state:	LOAD	TEST	RUN

Note: State **PERS** is not available in Compact or Enhanced BasicCards, so it is not allowed here.

6. Plug-In Libraries

In Terminal programs and Enhanced and Professional BasicCard programs, the functionality of the ZC-Basic language can be extended using ZeitControl Plug-In Libraries. For each Plug-In Library, we provide a definition file *library.def*. For the Enhanced BasicCard, a ZeitControl Library File *library.lib* is also provided. To use a library:

#Include library.def

This loads the library, and declares its procedures and data.

The following ZeitControl Plug-In Libraries are currently available:

<i>Name</i>	<i>Description</i>	<i>Terminal</i>	<i>Enhanced BasicCard</i>	<i>Professional BasicCard</i>
RSA	RSA Public-Key Cryptography	✓		✓
AES	Advanced Encryption Standard	✓	✓	✓
EC-167	167-bit Elliptic Curve Cryptography	✓		✓
EC-161	161-bit Elliptic Curve Cryptography	✓	✓	
SHA-1	Secure Hash Algorithm, revision 1	✓	✓	✓
IDEA	International Data Encryption Algorithm	✓	✓	
MATH	Mathematical functions	✓		
MISC	Miscellaneous procedures	✓	✓	✓

These libraries are supplied with the distribution kit, in the BasicCardPro\Lib directory. The program **LIBVER**, in the same directory, displays the name and version number of a ZeitControl Plug-In Library file.

In the descriptions of the individual libraries, error codes may be defined. These error codes are signalled via the **LibError** variable. The **ZCMBASIC** compiler automatically declares this variable if any libraries are included that can return an error code. **LibError** contains the most recent error code signalled by a library procedure. A library procedure never sets **LibError** back to zero; if you want to continue after detecting a library error, you should set **LibError** to zero yourself.

A library error code is always a 2-byte value of the form &H4XXX, with the high nibble equal to 4. Therefore, unless you are using the **T=0** protocol (and at the cost of strict ISO compatibility), you can return **LibError** in the **SW1SW2** status word if a library error is signalled in a BasicCard program. For example:

```
Sub CheckLibError()
  If LibError 0 Then Exit Sub
  SW1SW2 = LibError
  LibError = 0 ' Reset LibError for the next command
  Exit
End Sub
```

6.1 RSA: The Rivest-Shamir-Adleman Library

The **RSA** library implements Rivest-Shamir-Adleman public-key cryptography. It is based on the document **PKCS #1 v2.0: RSA Cryptography Standard** from RSA Data Security, Inc. The following operations are supported:

- on-card private/public key pair generation, with public key length up to 1024 bits;
- encryption and decryption;
- digital signature generation and verification.

6. Plug-In Libraries

6.1.1 Overview

In the **RSA** Plug-In Library, a private key consists of three numbers (p , q , e), where p and q are prime numbers and e is a number relatively prime to $p-1$ and $q-1$. The corresponding public key consists of the two numbers (n , e), where n is the product of p and q .

The private exponent d is the inverse of e modulo $(p-1)(q-1)$. Mathematically, this means that for any number m , m^{ed} is equal to m modulo n . If Alice wants to send a message m to Bob that only Bob can decrypt, Alice computes $c = m^e$ modulo n using Bob's public key (n_B , e_B). Bob can then recover m modulo n (and therefore m , if m is less than n), as follows:

- using p and q , compute the private exponent d ;
- compute $m = c^d$ modulo n .

Similarly, if Alice wants to sign a message m , she computes the private exponent d using her own private key (p_A , q_A , e_A), and then computes the signature $s = m^d$ modulo n . Anyone who has Alice's public key (n_A , e_A) can verify that $s^e = m$ modulo n ; and therefore that whoever created the signature s had knowledge of Alice's private key (and was therefore presumably Alice herself).

The security of the **RSA** system rests on the difficulty of recovering p and q if only their product n is known: the *factorisation problem*. If I know n and e , but I don't know p and q , then I can't calculate the private exponent d . The difficulty of the factorisation problem depends on the size of n . Current state-of-the-art factoring methods can factor a 512-bit public key in a matter of months; 768-bit public keys are expected to resist factorisation for a few more years; and 1024-bit keys are expected to be secure for the foreseeable future.

The **RSA** Plug-In Library represents large integers as ZC-Basic strings; the first byte in the string (with subscript 1) is the most significant byte.

To load the **RSA** library:

#Include RSA.DEF

The file RSA.DEF is supplied with the distribution kit, in the BasicCardPro\Lib directory.

The following procedures are provided:

```
Function RsaPseudoPrime (x$, nRounds)
Sub RsaGenerateKey (nBits, eBits, p$, q$, e$)
Function RsaPublicKey (p$, q$) As String
Sub RsaEncrypt (Mess$, n$, e$)
Sub RsaDecrypt (Mess$, p$, q$, e$)
Sub RsaPKCS1Sign (Hash$, p$, q$, e$, Sig$)
Function RsaPKCS1Verify (Hash$, n$, e$, Sig$)
Sub RsaPKCS1Encrypt (Mess$, n$, e$)
Function RsaPKCS1Decrypt (Mess$, p$, q$, e$)
Sub RsaOAEPDecrypt (Mess$, EP$, n$, e$)
Function RsaOAEPDecrypt (Mess$, EP$, p$, q$, e$)
```

These procedures are described in the following sections.

6.1.2 Key Generation

To generate a private key:

Call RsaGenerateKey (nBits, eBits, p\$, q\$, e\$)

<i>nBits</i>	Length of public key n . Set $nBits = 1024$ for maximum security. In a BasicCard program, $nBits$ must be a multiple of 16, with $496 \leq nBits \leq 1024$. In a Terminal program, $nBits$ can be any number between 16 and 4096.
<i>eBits</i>	Length of public exponent e . In a BasicCard program, $eBits$ must be a multiple of 8, with $8 \leq eBits \leq 32$. In a Terminal program, $eBits$ can be any number between 8 and 2032. If $nBits$ is 1024, we recommend $eBits = 32$.
<i>p\$, q\$, e\$</i>	The private key (p , q , e).

RsaGenerateKey uses the Rabin-Miller primality test, as described in **IEEE P1363: Standard Specifications for Public Key Cryptography**. The number of Rabin-Miller rounds depends on *nBits*; it is chosen so that the probability of a given factor being composite is less than 1 in 2^{100} .

The following error codes are returned in the **LibError** variable:

RsaKeyTooShort	In a BasicCard program: <i>nBits</i> < 496. In a Terminal program: <i>nBits</i> < 16.
RsaKeyTooLong	In a BasicCard program: <i>nBits</i> > 1024. In a Terminal program: <i>nBits</i> > 4064.
RsaBadProcParams	In a BasicCard program: <i>nBits</i> is not a multiple of 16, or <i>eBits</i> is not a multiple of 8, or <i>eBits</i> < 8, or <i>eBits</i> > 32. In a Terminal program: <i>eBits</i> < 8, or <i>eBits</i> > 2032.

To calculate the public key modulus *n* from *p* and *q*:

n\$ = **RsaPublicKey** (*p*\$, *q*\$)

The following error code is returned in the **LibError** variable:

RsaKeyTooLong	In a BasicCard program: <i>p</i> \$ or <i>q</i> \$ longer than 512 bits. In a Terminal program: <i>n</i> \$ longer than 2032 bits.
----------------------	---

If you want to generate your own random numbers *p*\$ and *q*\$, you can test them for primality with:

IsPrime = **RsaPseudoPrime** (*x*\$, *nRounds*)

<i>x</i> \$	Number to test for primality.
<i>nRounds</i>	Number of rounds of Rabin-Miller primality test to run.
<i>IsPrime</i>	True if <i>x</i> \$ survives <i>nRounds</i> rounds of the Rabin-Miller primality test.

6.1.3 Cryptographic Primitives

Four cryptographic primitives are defined in **PKCS #1 v2.0: RSA Cryptography Standard**:

RSAEP ((<i>n</i> , <i>e</i>), <i>m</i>)	RSA Encryption Primitive: $c = m^e$ modulo <i>n</i>
RSADP ((<i>n</i> , <i>d</i>), <i>c</i>)	RSA Decryption Primitive: $m = c^d$ modulo <i>n</i>
RSASP1 ((<i>n</i> , <i>d</i>), <i>c</i>)	RSA Signature Primitive 1: $s = m^d$ modulo <i>n</i>
RSAPV1 ((<i>n</i> , <i>e</i>), <i>s</i>)	RSA Verification Primitive 1: $m = s^e$ modulo <i>n</i>

RSAEP and **RSAPV1** are functionally identical, as are **RSADP** and **RSASP1**. The **RSA** Plug-In Library provides two procedures.

Cryptographic primitives RSAEP and RSAPV1

Call RsaEncrypt (*Mess*\$, *n*\$, *e*\$)

This procedure computes *Mess*\$^{*e*\$} modulo *n*\$, returning the result in *Mess*\$.

In a BasicCard program, the following error codes are returned in the **LibError** variable:

RsaKeyTooShort	<i>n</i> \$ is shorter than 248 bits
RsaKeyTooLong	<i>n</i> \$ is longer than 1024 bits
RsaBadProcParams	<i>Mess</i> \$ is longer than 1024 bits

Cryptographic primitives RSADP and RSASP1

Call RsaDecrypt (*Mess*\$, *p*\$, *q*\$, *e*\$)

This procedure first computes *d*\$ = inverse of *e*\$ modulo (*p*\$-1)(*q*\$-1). Then it computes *Mess*\$^{*d*\$} modulo *p*\$ *q*\$, returning the result in *Mess*\$.

In a BasicCard program, the following error codes are returned in the **LibError** variable:

RsaKeyTooShort	<i>p</i> \$ or <i>q</i> \$ is shorter than 248 bits
RsaKeyTooLong	<i>p</i> \$ or <i>q</i> \$ is longer than 512 bits
RsaBadProcParams	<i>Mess</i> \$ is longer than 1024 bits

6. Plug-In Libraries

6.1.4 Signature Scheme With Appendix

As described in **PKCS #1 v2.0: RSA Cryptography Standard**, a *signature scheme with appendix* consists of a *signature generation operation* and a *signature verification operation*. One signature scheme with appendix is defined: **RSASSA-PKCS1-v1_5**.

The **RSA** Plug-In Library uses **SHA-1** as the hash function for the signature scheme. **6.5 SHA-1: The Secure Hash Algorithm Library** describes how to calculate 20-byte hash values using **SHA-1**.

To generate a signature using the **RSASSA-PKCS1-v1_5-SIGN** signature generation operation:

Call RsaPKCS1Sign (*Hash*\$, *p*\$, *q*\$, *e*\$, *Sig*\$)

<i>Hash</i> \$	The 20-byte SHA-1 hash of the data to be signed.
<i>p</i> \$, <i>q</i> \$, <i>e</i> \$	The private key (<i>p</i> , <i>q</i> , <i>e</i>).
<i>Sig</i> \$	The signature calculated by RsaPKCS1Sign . It has the same size as <i>n</i> \$ (where $n = pq$ is the public-key modulus).

The following error codes are returned in the **LibError** variable:

RsaKeyTooShort	<i>n</i> \$ is shorter than 376 bits
RsaBadProcParams	<i>Hash</i> \$ is not 20 bytes long

To verify a signature using the **RSASSA-PKCS1-v1_5-VERIFY** signature verification operation:

SignatureValid = **RsaPKCS1Verify** (*Hash*\$, *n*\$, *e*\$, *Sig*\$)

<i>Hash</i> \$	The 20-byte SHA-1 hash of the data that was signed.
<i>n</i> \$, <i>e</i> \$	The private key (<i>n</i> , <i>e</i>).
<i>Sig</i> \$	The signature to be verified.
<i>SignatureValid</i>	True if the signature is valid.

The following error codes are returned in the **LibError** variable:

RsaKeyTooShort	<i>n</i> \$ is shorter than 376 bits
RsaBadProcParams	<i>Hash</i> \$ is not 20 bytes long

6.1.5 Encryption Schemes

As described in **PKCS #1 v2.0: RSA Cryptography Standard**, an *encryption scheme* consists of an *encryption operation* and a *decryption operation*. Two encryption schemes are defined: **RSAES-PKCS1-v1_5** and **RSAES-OAEP**. The second of these is cryptographically more robust, but is bigger and slower; it is currently only available in Terminal programs.

The **RSA** Plug-In Library uses **SHA-1** as the hash function for the encryption schemes. **6.5 SHA-1: The Secure Hash Algorithm Library** describes how to calculate 20-byte hash values using **SHA-1**.

The **RSAES-PKCS1-v1_5** Encryption Scheme

To encrypt a message using the **RSAES-PKCS1-v1_5-ENCRYPT** encryption operation:

Call RsaPKCS1Encrypt (*Mess*\$, *n*\$, *e*\$)

<i>Mess</i> \$	The message to be encrypted. It must be at least 11 bytes shorter than <i>n</i> \$. The encrypted message is returned in <i>Mess</i> \$.
<i>n</i> \$, <i>e</i> \$	The public key (<i>n</i> , <i>e</i>).

The following error code is returned in the **LibError** variable:

RsaBadProcParams	<i>Mess</i> \$ is not at least 11 bytes shorter than <i>n</i> \$.
-------------------------	---

To decrypt a message using the **RSAES-PKCS1-v1_5-DECRYPT** decryption operation:

MessageValid = **RsaPKCS1Decrypt** (*Mess*\$, *p*\$, *q*\$, *e*\$)

<i>Mess</i> \$	The message to be decrypted. It must be the same length as <i>n</i> \$ (where $n = pq$ is the public-key modulus). The decrypted message is returned in <i>Mess</i> \$.
<i>p</i> \$, <i>q</i> \$, <i>e</i> \$	The private key (<i>p</i> , <i>q</i> , <i>e</i>).
<i>MessageValid</i>	True if <i>Mess</i> \$ was successfully decrypted.

6.2 AES: The Advanced Encryption Standard Library

The following error code is returned in the **LibError** variable:

RsaBadProcParams *Mess\$* is not the same size as *n\$*.

The **RSAES-OAEP** Encryption Scheme

The **RSAES-OAEP** scheme accepts *encoding parameters* as input. The same encoding parameters must be specified for encryption and decryption. The encoding parameters can be any arbitrary string, and need not be secret; if in doubt, use the empty string "".

To encrypt a message using the **RSAES-OAEP-ENCRYPT** operation (Terminal programs only):

Call RsaOAEPDecrypt (*Mess\$, EP\$, n\$, e\$*)

Mess\$ The message to be encrypted. It must be at least 42 bytes shorter than *n\$*. The encrypted message is returned in *Mess\$*.

EP\$ The encoding parameters. Any string is accepted.

n\$, e\$ The public key (*n*, *e*).

The following error code is returned in the **LibError** variable:

RsaBadProcParams *Mess\$* is not at least 42 bytes shorter than *n\$*.

To decrypt a message using the **RSAES-OAEP-DECRYPT** operation (Terminal programs only):

MessageValid = **RsaOAEPDecrypt** (*Mess\$, EP\$, p\$, q\$, e\$*)

Mess\$ The message to be decrypted. It must be the same length as *n\$* (where $n = pq$ is the public-key modulus). The decrypted message is returned in *Mess\$*.

EP\$ The encoding parameters. They must match the *EP\$* parameter to the **RsaOAEPDecrypt** procedure.

p\$, q\$, e\$ The private key (*p*, *q*, *e*).

MessageValid **True** if *Mess\$* was successfully decrypted.

The following error code is returned in the **LibError** variable:

RsaBadProcParams *Mess\$* is not the same size as *n\$*.

6.2 AES: The Advanced Encryption Standard Library

This library implements the Advanced Encryption Standard defined in Federal Information Processing Standard FIPS 197. This standard is available on the Internet, at <http://csrc.nist.gov/encryption/aes/>. **AES** uses the Rijndael algorithm as its cryptographic primitive. The Standard specifies three permitted key lengths: 128 bits, 192 bits, and 256 bits. All three key lengths are available to Terminal programs. At the time of writing, Professional BasicCard **ZC5.5** supports all three key lengths; other versions of the BasicCard are restricted to 128-bit keys.

To load this library:

#Include AES.DEF

The file AES.DEF is supplied with the distribution kit, in the BasicCardPro\Lib directory.

The **AES** library consists of a single procedure:

Function AES (*Type%, Key\$, Block\$*) **As String**

This function encrypts or decrypts the 16-byte *Block\$* with the given *Key\$*, according to the *Type%* parameter:

<i>Type%</i>	
128	Encryption with 128-bit key. Len (<i>Key\$</i>) must be ≥ 16 .
192	Encryption with 192-bit key. Len (<i>Key\$</i>) must be ≥ 24 .
256	Encryption with 256-bit key. Len (<i>Key\$</i>) must be ≥ 32 .
-128	Decryption with 128-bit key. Len (<i>Key\$</i>) must be ≥ 16 .
-192	Decryption with 192-bit key. Len (<i>Key\$</i>) must be ≥ 24 .
-256	Decryption with 256-bit key. Len (<i>Key\$</i>) must be ≥ 32 .

6. Plug-In Libraries

The return value of the function is the encrypted or decrypted *Block\$*. If *Block\$* is shorter than 16 bytes, it is padded with zeroes before encryption/decryption; if it is longer than 16 bytes, it is truncated before encryption/decryption. In any case, the contents of the original *Block\$* are unchanged.

The following error codes are returned in the **LibError** variable:

AesBadType	<i>Type%</i> is not ± 128 , ± 192 , or ± 256 .
AesUnsupportedType	<i>Type%</i> is ± 192 or ± 256 , but the key length is not supported.
AesKeyTooShort	<i>Key\$</i> is shorter than 16/24/32 bytes.

6.3 EC-167: The 167-Bit Elliptic Curve Library

The **EC-167** library implements Elliptic Curve Cryptography over the field $GF(2^{167})$, with 167-bit keys. This library is available for Terminal programs and the Series 5 Professional BasicCard; the Enhanced BasicCard uses the **EC-161** library. See **6.3.1 Field Exponents** for a discussion of the differences between the two libraries.

The following operations are supported:

- private/public key pair generation;
- session key generation;
- digital signature generation;
- digital signature verification.

This implementation follows the standard **IEEE P1363: Standard Specifications for Public Key Cryptography**. Section **6.3.10 Conformance Specification** specifies the methods used in library **EC-167**, using the terminology of **IEEE P1363**.

A simple Elliptic Curve application can be found in the directory `BasicCardPro\Examples\EC`.

6.3.1 Field Exponents

Two Elliptic Curve libraries are available for the BasicCard: **EC-167** for the Series 5 Professional BasicCard, and **EC-161** for the Enhanced BasicCard. **EC-167** implements Elliptic Curve Cryptography over the field $GF(2^{167})$, with 167-bit keys; **EC-161** implements Elliptic Curve Cryptography over the field $GF(2^{168})$, with 161-bit keys.

The important difference between these two libraries is not the key length (167 vs. 161), but the field exponent (167 vs. 168). This section explains the significance of the field exponent.

In a Smart Card implementation of Elliptic Curve Cryptography, arithmetic over the underlying field must be made as fast as possible. Certain field exponents allow ingenious short cuts, speeding up the arithmetic significantly. One such exponent is 168, as used by **EC-161**. Our implementation achieves a speed-up factor of five or six; without this speed-up, Elliptic Curve Cryptography in the Enhanced BasicCard would be too slow for practical use.

However, the latest consensus among experts is that the field exponent should be a prime number, such as 167; certain composite exponents have been shown to be cryptographically weak, and the feeling is that all composite exponents (for example, 168) should therefore be avoided.

The processor in the Series 5 Professional BasicCard is twelve times as fast as the Enhanced BasicCard. So the **EC-167** library in the Professional BasicCard is twice as fast as the **EC-161** library in the Enhanced BasicCard, although it is doing five or six times as much work. This lets us offer two Elliptic Curve Cryptography solutions:

- **EC-167** for applications that require high security over an extended period of time;
- **EC-161** for applications that are short-lived, or have only low-value information to protect.

6.3.2 Elliptic Curve Cryptography

Elliptic Curve Cryptography is a branch of Public Key Cryptography that is especially suitable for Smart Card implementation, for (at least) two reasons:

6.3 EC-167: The 167-Bit Elliptic Curve Library

- the generation of private/public key pairs is simple enough to be implemented in a Smart Card;
- it requires much smaller key sizes than other well-known methods for the same level of security.

The library **EC-167** uses points with 167-bit prime order; this is currently considered equivalent in security to 1024-bit RSA.

To load the Elliptic Curve library:

```
#Include EC-167.DEF
```

The file EC-167.DEF is supplied with the distribution kit, in the `BasicCardPro\Lib` directory.

6.3.3 Setting the Elliptic Curve Parameters

An Elliptic Curve is defined by its EC Domain Parameters; five suitable Elliptic Curves are supplied in the directory `BasicCardPro\Lib\Curves`. Choose one of these for your application. Twenty *Curve Definition Files* EC167-1.16 through EC167-5.128 contain curve definitions in ZC-Basic, for inclusion in a source program. File EC-167.BIN contains the binary data for all five curves, for run-time loading in a Terminal program.

To specify an Elliptic Curve in a Professional BasicCard program:

```
#Include Curves\EC167-X.N
```

where *X* is a number from 1 to 5, and *N* is a power of 2 between 16 and 128. In a BasicCard program, the curve must be chosen at compile time; it can't be re-loaded at run-time. This Curve Definition File loads *N* pre-computed Elliptic Curve points into EEPROM to speed up Elliptic Curve operations. The more pre-computed points, the faster the card, but the less free EEPROM space. If EEPROM space is at a premium, use 16 pre-computed points; if speed is the most important factor, use 128 pre-computed points.

In the Terminal program, an Elliptic Curve must be explicitly loaded using **EC167SetCurve**. There are three ways of doing this:

- If you know in advance which curve to use, you can include its definition file. For example:

```
#Include EC167-3.16
Call EC167SetCurve (EC167Params)
```

But note that only one such definition file is allowed in a program.

- If the card has a suitable command, you can load the curve from the card. For example:

```
Private Curve As EC167DomainParams
Call GetCurve (Curve) : Call CheckSW1SW2()
Call EC167SetCurve (Curve)
```

See `BasicCardPro\Examples\EC` for an example of this.

- You can read the curve from the binary file EC-167.BIN. For example:

```
Private Curve As EC167DomainParams
Open "EC-167.BIN" For Random As #1 Len=64
Get #1, 3, Curve ' Read Elliptic Curve #3
Close #1
Call CheckFileError()
Call EC167SetCurve (Curve)
```

If the EC domain parameters are invalid, procedure **EC167SetCurve** returns error code **EC167BadCurveParams** in variable **LibError**.

In the Terminal program, you must call **EC761SetCurve** before you call any other procedures from the **EC-167** library. If not, error code **EC167CurveNotInitialised** will be returned in variable **LibError**.

6.3.4 Key Generation

To generate a public/private key pair:

```
Call EC167GenerateKeyPair()
```


6. Plug-In Libraries

This procedure generates a random 21-byte private key and its associated 21-byte public key, storing them in **Eeprom** strings **EC167PrivateKey** and **EC167PublicKey**. In a Professional BasicCard with 128 pre-computed points, this subroutine takes about 0.6 seconds.

6.3.5 Setting an Explicit Private Key

To set an explicit value for a private key:

Call EC167SetPrivateKey (Key\$)

This procedure copies *Key\$* (reduced modulo *r*) to the 21-byte **Eeprom** string **EC167PrivateKey**, and computes the associated 21-byte **Eeprom** string **EC167PublicKey**. (*r* is explained in **6.3.9 Binary Representation Formats: EC Domain Parameters**.) In a Professional BasicCard with 128 pre-computed points, this subroutine takes about 0.6 seconds.

If *Key\$* is zero modulo *r*, error code **EC167BadProcParams** is returned in variable **LibError**.

6.3.6 Generating a Digital Signature

A private key is used to generate digital signatures. To sign a message consisting of a **String** expression:

Call EC167HashAndSign (Signature\$, Message\$)

This procedure returns a 42-byte string in *Signature\$*.

To sign a longer message, first compute the hash function for the message (see **6.5.1 Hashing Functions**), and then

Call EC167Sign (Signature\$, Hash\$)

If no private key has been set, these procedures return error code **EC167KeyNotInitialised** in variable **LibError**.

In a Professional BasicCard with 128 pre-computed points, this subroutine takes about 0.65 seconds.

6.3.7 Verifying a Digital Signature

Note: Verification of Digital Signatures is only possible in a Terminal program, or in Professional BasicCard **ZC5.5**. At the time of writing, it is not supported in other Professional BasicCards.

To verify a digital signature, you need the signer's public key. To verify the signature of a message consisting of a **String** expression:

Status = EC167HashAndVerify (Signature\$, Message\$, PublicKey\$)

<i>Signature\$</i>	The 42-byte signature to be verified
<i>Message\$</i>	The message that was signed
<i>PublicKey\$</i>	The signer's 21-byte public key

This function returns **True** or **False** according to whether the signature is valid or not.

To verify a longer message, first compute the hash function for the message (see **6.5.1 Hashing Functions**), and then verify its signature with the function:

Status = EC167Verify (Signature\$, Hash\$, PublicKey\$)

If *Signature\$* is not 42 bytes, or *PublicKey\$* is not 21 bytes, error code **EC167BadProcParams** is returned in variable **LibError**.

6.3.8 Session Key Generation

If two parties know each other's public keys, they can use them to agree on a secret 21-byte value. This value is called the *shared secret* for the two parties; to compute it, you need to know the private key of one party (in **EC167PrivateKey**) and the public key of the other party. To compute the shared secret:

SharedSecret\$ = EC167SharedSecret (PublicKey\$)

<i>PublicKey\$</i>	The other party's 21-byte public key
<i>SharedSecret\$</i>	The 21-byte shared secret

If *PublicKey\$* is not 21 bytes long, or it is not a point on the curve, error **EC167BadProcParams** is returned in variable **LibError**.

This shared secret can then be used to generate 20-byte session keys for encrypting messages between the two parties; unlike the shared secret, a session key can be different on different occasions.

To generate a session key, the parties must agree on a *Key Derivation Parameter*, which can be any sequence of bytes, and need not be kept secret. For maximum security, it should be different each time a session key is generated. For example, it might be a standard header followed by the date and time. To generate the session key:

SessionKey\$ = **EC167SessionKey** (*KDP\$*, *SharedSecret\$*)

KDP\$ Key Derivation Parameter, a string of any length
SharedSecret\$ The shared secret value, returned by **EC167SharedSecret**
SessionKey\$ The 20-byte session key

Note: In the Professional BasicCard, generating a shared secret takes about 2.7 seconds. But once a shared secret has been generated for a given public key, session key generation takes less than 0.1 seconds, provided **Len(KDP\$)** <= 42. (Typically, a smart card application will only need to generate session keys for a single public key, for which the shared secret is computed just once in the card's lifetime.)

6.3.9 Binary Representation Formats

This section specifies the binary representations of the data objects that are used in the library: integers, field elements, elliptic curves, points on the curve, and signatures.

Integers

Integers in this implementation have a length of either 1 byte or 21 bytes. The first (or leftmost) byte is the most significant – in a 21-byte integer, it contains bits 167-160. The last (or rightmost) byte contains bits 7-0.

Field Elements

The library **EC-167** implements operations on Elliptic Curves over the field **GF(2^m)**, with *m* = 167. An element of **GF(2^m)** is represented by 167 bits stored in 21 bytes. A Polynomial Basis field representation is used; the Field Polynomial is

$$p(t) = t^{167} + t^6 + 1$$

The first (leftmost) byte contains the coefficients of t^{166} through t^{160} .

EC Domain Parameters

An Elliptic Curve *E* over **GF(2^m)** is defined by an equation of the form

$$y^2 + xy = x^3 + ax^2 + b$$

where *a* and *b* are elements of **GF(2^m)** with *b* ≠ 0. The curve *E* consists of all points (*x*, *y*) with *x*, *y* ∈ **GF(2^m)** that satisfy this equation, together with a *Point at Infinity*, denoted **O**. The order *#E* of the curve is the number of points in *E*. For cryptographic purposes, this order must have a large prime divisor, i.e. *#E* = *kr* for some (large) prime *r*. As well as *a*, *b*, *r*, and *k*, a point *G* ∈ *E* must be specified, of order *r* (that is, *r* is the smallest positive integer such that *rG* = **O**.) Field elements *a* and *b* ∈ **GF(2^m)**, integers *r* and *k*, and point *G* ∈ *E* constitute the *EC domain parameters*.

The library **EC-167** accepts any set of EC domain parameters (*a*, *b*, *r*, *k*, *G*) that satisfies the following conditions:

- *a* is zero in all bit positions except for bits 7-0 ;
- *r* is exactly 167 bits long, i.e. $2^{166} < r < 2^{167}$;
- *k* is equal to 2.

The user-defined type **EC167DomainParams**, defined in file `BasicCardPro\Lib\EC-167.DEF`, contains curve parameters *a* (1 byte), *b* (21 bytes), *r* (21 bytes), and *G* (21 bytes), for a total of 64 bytes.

6. Plug-In Libraries

Points on the Curve

Points on the curve play two roles in library **EC-167**:

- EC domain parameter G is a point on the curve;
- every public key is a point on the curve. (For a private key s , the corresponding public key is sG .)

If P is on the curve and $x_P \neq 0$, then $y^2 + x_P y = x_P^3 + ax_P^2 + b$ has two solutions, y_0 and y_1 . Moreover, the two expressions y_0/x_P and y_1/x_P differ only in bit 0; so if we know x_P and bit 0 of y_P/x_P , we can recover point P in full. This bit is called the *compressed y-coordinate* of the point P , denoted \tilde{y}_P . A point P on the curve is represented by 21 bytes, with \tilde{y}_P in bit 167, and x_P in bits 166-0.

Signatures

A signature consists of two 21-byte integers (c, d) . See **IEEE P1363** for the definitions of c and d .

6.3.10 Conformance Specification

This implementation follows the standard **IEEE P1363: Standard Specifications for Public Key Cryptography**. In the terminology of this standard, the following schemes, primitives, and additional techniques are implemented:

<i>Scheme</i>	<i>Description</i>	<i>Terminal</i>	<i>Professional BasicCard</i>
ECKAS-DH1	Elliptic Curve Key Agreement Scheme, Diffie-Hellman version, where each party contributes one key pair. This scheme uses primitive ECSVDP-DH , with additional technique KDF1 .	✓	✓
ECSSA	Elliptic Curve Signature Scheme with Appendix. This scheme uses primitives ECSP-NR (in the Terminal and the BasicCard) and ECSV-NR (in the Terminal only), and additional technique EMSA1 .	✓	✓

<i>Primitive</i>	<i>Description</i>	<i>Terminal</i>	<i>Professional BasicCard</i>
ECSVDP-DH	Elliptic Curve Secret Value Derivation Primitive, Diffie-Hellman version.	✓	✓
ECSP-NR	Elliptic Curve Signature Primitive, Nyberg-Rueppel version.	✓	✓
ECVP-NR	Elliptic Curve Verification Primitive, Nyberg-Rueppel version.	✓	ZC5.5

<i>Additional Technique</i>	<i>Description</i>	<i>Terminal</i>	<i>Professional BasicCard</i>
KDF1	Key Derivation Function. The hash function is SHA-1: Secure Hash Algorithm, revision 1 .	✓	✓
EMSA1	Encoding Method for Signatures with Appendix. The hash function is SHA-1: Secure Hash Algorithm, revision 1 .	✓	✓

6.4 EC-161: The 161-Bit Elliptic Curve Library

The **EC-161** library implements Elliptic Curve Cryptography over the field $GF(2^{168})$, with 161-bit keys. This library is available for Terminal programs and Enhanced BasicCard programs. The **EC-167** library is available for Series 5 Professional BasicCards; see **6.3 EC-167: The 167-Bit Elliptic Curve Library** for more information.

The following operations are supported:

- private/public key pair generation;
- session key generation;
- digital signature generation;
- digital signature verification (Terminal program only).

This implementation follows the proposed standard **IEEE P1363: Standard Specifications for Public Key Cryptography**. Section **6.4.8 Conformance Specification** specifies the methods used in library **EC-161**, using the terminology of **IEEE P1363**.

A simple Elliptic Curve application can be found in the directory `BasicCardPro\Examples\EC`.

To load the Elliptic Curve library:

```
#Include EC-161.DEF
```

The file `EC-161.DEF` is supplied with the distribution kit, in the `BasicCardPro\Lib` directory.

6.4.1 Setting the Elliptic Curve Parameters

An Elliptic Curve is defined by its EC Domain Parameters; three suitable Elliptic Curves are supplied in the directory `BasicCardPro\Lib\Curves`. Choose one of these for your application. *Curve Definition Files* `EC161-1.CRV` through `EC161-3.CRV` contain curve definitions in ZC-Basic, for inclusion in a source program. File `EC-161.BIN` contains the binary data for all three curves, for run-time loading in a Terminal program.

To specify an Elliptic Curve in an Enhanced BasicCard program:

```
#Include EC161-X.CRV
```

where *X* is a number from 1 to 3. In a BasicCard program, the curve must be chosen at compile time; it can't be re-loaded at run-time. In Enhanced BasicCards without the **EC-FSA** algorithm, this Curve Definition File loads 32 pre-computed Elliptic Curve points into EEPROM to speed up Elliptic Curve operations. We also provide Curve Definition Files **EC161-X.16** and **EC161-X.64**, with 16 and 64 pre-computed points respectively. The more pre-computed points, the faster the card, but the less free EEPROM space. If EEPROM space is at a premium, use 16 pre-computed points; if speed is the most important factor, use 64 pre-computed points. (The **EC-FSA** algorithm doesn't use these pre-computed points, so there is no difference between these Curve Definition Files for **EC-FSA** cards.)

In the Terminal program, an Elliptic Curve must be explicitly loaded using **EC161SetCurve**. There are three ways of doing this:

- If you know in advance which curve to use, you can include its definition file. For example:

```
#Include EC161-3.CRV
Call EC161SetCurve (EC161Params)
```

But note that only one such definition file is allowed in a program.

- If the card has a suitable command, you can load the curve from the card. For example:

```
Private Curve As EC161DomainParams
Call GetCurve (Curve) : Call CheckSW1SW2()
Call EC161SetCurve (Curve)
```

See `BasicCardPro\Examples\EC` for an example of this.

- You can read the curve from the binary file `EC-161.BIN`. For example:

```
Private Curve As EC161DomainParams
Open "EC-161.BIN" For Random As #1 Len=64
Get #1, 3, Curve ' Read Elliptic Curve #3
Close #1
Call CheckFileError()
Call EC161SetCurve (Curve)
```

If the EC domain parameters are invalid, procedure **EC161SetCurve** returns error code **EC161BadCurveParams** in variable **LibError**.

6. Plug-In Libraries

In the Terminal program, you must call **EC161SetCurve** before you call any other procedures from the **EC-161** library. If not, error code **EC161CurveNotInitialised** will be returned in variable **LibError**.

6.4.2 Key Generation

To generate a public/private key pair:

Call EC161GenerateKeyPair (Seed\$)

This procedure uses library **SHA-1** to generate a cryptographically strong pseudo-random number from *Seed\$*, for use as a private key. The 21-byte private key and its associated 22-byte public key are stored in **Eeprom** strings **EC161PrivateKey** and **EC161PublicKey**.

See **6.5.2 Pseudo-Random Number Generation** for more about pseudo-random numbers in **SHA-1**.

6.4.3 Setting an Explicit Private Key

To set an explicit value for a private key:

Call EC161SetPrivateKey (Key\$)

This procedure copies *Key\$* (reduced modulo *r*) to the 21-byte **Eeprom** string **EC161PrivateKey**, and computes the associated 22-byte **Eeprom** string **EC161PublicKey**. (*r* is explained in **6.4.7 Binary Representation Formats: EC Domain Parameters**.)

If *Key\$* is zero modulo *r*, error code **EC161BadProcParams** is returned in variable **LibError**.

Note: In the BasicCard, this procedure takes about 4 seconds to execute at a clock speed of 3.57 MHz. However, if you don't need to compute **EC161PublicKey**, you can simply copy *Key\$* to **EC161PrivateKey**, and the Elliptic Curve routines will work correctly.

6.4.4 Generating a Digital Signature

A private key is used to generate digital signatures. To sign a message consisting of a **String** expression:

Call EC161HashAndSign (Signature\$, Message\$)

This procedure returns a 42-byte string in *Signature\$*.

To sign a longer message, first compute the hash function for the message (see **6.5.1 Hashing Functions**), and then call

Call EC161Sign (Signature\$, Hash\$)

If no private key has been set, these procedures return error code **EC161KeyNotInitialised** in variable **LibError**.

In the regular Enhanced BasicCard, digital signature generation takes about 2.5 seconds at a clock speed of 3.57 MHz. In Enhanced BasicCards ZC3.5 and ZC3.6 with **EC-FSA**, it takes about 1.2 seconds.

6.4.5 Verifying a Digital Signature

Note: Verification of Digital Signatures is only possible in a Terminal program. It is not supported in the Enhanced BasicCard.

To verify a digital signature, you need the signer's public key. To verify the signature of a message consisting of a **String** expression:

Status = **EC161HashAndVerify (Signature\$, Message\$, PublicKey\$)**

<i>Signature\$</i>	The 42-byte signature to be verified
<i>Message\$</i>	The message that was signed
<i>PublicKey\$</i>	The signer's 22-byte public key

This function returns **True** or **False** according to whether the signature is valid or not.

To verify a longer message, first compute the hash function for the message (see **6.5.1 Hashing Functions**), and then verify its signature with the function:

Status = **EC161Verify** (*Signature*\$, *Hash*\$, *PublicKey*\$)

If *Signature*\$ is not 42 bytes, or *PublicKey*\$ is not 22 bytes, error code **EC161BadProcParams** is returned in variable **LibError**.

6.4.6 Session Key Generation

If two parties know each other's public keys, they can use them to agree on a secret 21-byte value. This value is called the *shared secret* for the two parties; to compute it, you need to know the private key of one party (either one will do) and the public key of the other party. To compute the shared secret:

SharedSecret\$ = **EC161SharedSecret** (*PublicKey*\$)

PublicKey\$ The other party's 22-byte public key

SharedSecret\$ The 21-byte shared secret

If *PublicKey*\$ is not 22 bytes long, or it is not a point on the curve, error **EC161BadProcParams** is returned in variable **LibError**.

This shared secret can then be used to generate 20-byte session keys for encrypting messages between the two parties; unlike the shared secret, a session key can be different on different occasions.

To generate a session key, the parties must agree on a *Key Derivation Parameter*, which can be any sequence of bytes, and need not be kept secret. For maximum security, it should be different each time a session key is generated. For example, it might be a standard header followed by the date and time. To generate the session key:

SessionKey\$ = **EC161SessionKey** (*KDP*\$, *SharedSecret*\$)

KDP\$ Key Derivation Parameter, a string of any length

SharedSecret\$ The shared secret value, returned by **EC161SharedSecret**

SessionKey\$ The 20-byte session key

Note: In the BasicCard, generating a shared secret takes about 7 seconds at a clock speed of 3.57 MHz. But once a shared secret has been generated for a given public key, session key generation takes less than half a second at the same clock speed, provided **Len(KDP\$)** <= 42. (Typically, a smart card application will only need to generate session keys for a single public key, for which the shared secret is computed just once in the card's lifetime.)

6.4.7 Binary Representation Formats

This section specifies the binary representations of the data objects that are used in the library: integers, field elements, elliptic curves, points on the curve, and signatures.

Integers

Integers in this implementation have a length of either 1 byte or 21 bytes. The first (or leftmost) byte is the most significant – in a 21-byte integer, it contains bits 167-160. The last (or rightmost) byte contains bits 7-0.

Field Elements

The library **EC-161** implements operations on Elliptic Curves over the field **GF**(2^m), with m = 168. An element of **GF**(2^m) is represented by 168 bits stored in 21 bytes. The field representation is non-standard (i.e. it does not use a Polynomial Basis or a Normal Basis); for this reason we provide source code, in C and ZC-Basic, for converting between ZeitControl's EC-161 representation and a standard Polynomial Basis representation. This Polynomial Basis representation uses irreducible field polynomial

$$p(t) = t^{168} + t^{15} + t^3 + t^2 + 1$$

The source code is in directory BasicCardPro\Source\FldConv.

6. Plug-In Libraries

EC Domain Parameters

An Elliptic Curve E over $\mathbf{GF}(2^m)$ is defined by an equation of the form

$$y^2 + xy = x^3 + ax^2 + b$$

where a and b are elements of $\mathbf{GF}(2^m)$ with $b \neq 0$. The curve E consists of all points (x, y) with $x, y \in \mathbf{GF}(2^m)$ that satisfy this equation, together with a *Point at Infinity*, denoted O . The order $\#E$ of the curve is the number of points in E . For cryptographic purposes, this order must have a large prime divisor, i.e. $\#E = kr$ for some (large) prime r . As well as a, b, r , and k , a point $G \in E$ must be specified, of order r (that is, r is the smallest positive integer such that $rG = O$.) Field elements a and $b \in \mathbf{GF}(2^m)$, integers r and k , and point $G \in E$ constitute the *EC domain parameters*. (k is redundant, as it can be calculated from a, b , and r ; it is included for convenience.)

The library **EC-161** accepts any set of EC domain parameters (a, b, r, k, G) that satisfies the following conditions:

- a is zero in all bit positions except for bits 78-72 ;
- r is exactly 161 bits long, i.e. $2^{160} < r < 2^{161}$;
- k is a single byte, equal to 2 modulo 4.

The user-defined type **EC161DomainParams**, defined in file `BasicCardPro\Lib\EC-161.DEF`, contains curve parameters a (1 byte), b (21 bytes), r (21 bytes), k (1 byte), and G (22 bytes), for a total of 66 bytes.

Points on the Curve

Points on the curve play two roles in library **EC-161**:

- EC domain parameter G is a point on the curve;
- every public key is a point on the curve. (For a private key s , the corresponding public key is sG .)

If P is on the curve and $x_P \neq 0$, then $y^2 + x_P y = x_P^3 + ax_P^2 + b$ has two solutions, y_0 and y_1 . Moreover, the two expressions y_0/x_P and y_1/x_P differ only in bit 7 (in the representation used here); so if we know x_P and bit 7 of y_P/x_P , we can recover point P in full. This bit is called the *compressed y-coordinate* of the point P , denoted \tilde{y}_P . A point P on the curve is represented by 22 bytes, with x_P in the leftmost 21 bytes (i.e. bits 175-8), and the compressed y-coordinate \tilde{y}_P in bit 0.

Signatures

A signature consists of two 21-byte integers (c, d) . See **IEEE P1363** for the definitions of c and d .

6.4.8 Conformance Specification

This implementation follows the proposed standard **IEEE P1363 / D9 (Draft Version 9): Standard Specifications for Public Key Cryptography**. In the terminology of this standard, the following schemes, primitives, and additional techniques are implemented:

<i>Scheme</i>	<i>Description</i>	<i>Terminal</i>	<i>Enhanced BasicCard</i>
ECKAS-DH1	Elliptic Curve Key Agreement Scheme, Diffie-Hellman version, where each party contributes one key pair. This scheme uses primitive ECSVDP-DH , with additional technique KDF1 .	✓	✓
ECSSA	Elliptic Curve Signature Scheme with Appendix. This scheme uses primitives ECSP-NR (in the Terminal and the BasicCard) and ECSV-NR (in the Terminal only), and additional technique EMSA1 .	✓	✓

6.5 SHA–1: The Secure Hash Algorithm Library

<i>Primitive</i>	<i>Description</i>	<i>Terminal</i>	<i>Enhanced BasicCard</i>
ECSVDP-DH	Elliptic Curve Secret Value Derivation Primitive, Diffie-Hellman version.	✓	✓
ECSP-NR	Elliptic Curve Signature Primitive, Nyberg-Rueppel version.	✓	✓
ECVP-NR	Elliptic Curve Verification Primitive, Nyberg-Rueppel version.	✓	

<i>Additional Technique</i>	<i>Description</i>	<i>Terminal</i>	<i>Enhanced BasicCard</i>
KDF1	Key Derivation Function. The hash function is SHA–1: Secure Hash Algorithm, revision 1 .	✓	✓
EMSA1	Encoding Method for Signatures with Appendix. The hash function is SHA–1: Secure Hash Algorithm, revision 1 .	✓	✓

6.5 SHA–1: The Secure Hash Algorithm Library

This library implements the Secure Hash Algorithm as defined in the Federal Information Processing Standards document FIPS 180–1. The algorithm takes an arbitrary message as input, and outputs a 20-byte hash of that message. It is supposed to be computationally infeasible to invert this algorithm. More specifically:

- given a 20-byte hash, it is computationally infeasible to construct a message with that hash;
- it is computationally infeasible to construct two different messages with identical hashes.

FIPS 180-1 is available on the Internet, at www.itl.nist.gov/div897/pubs/fip180-1.htm.

The **SHA–1** library was implemented as an adjunct to the **RSA** and **EC–167** libraries. In the first place, it is specified in the proposed IEEE standard P1363 as one of the approved hashing algorithms for use in Elliptic Curve digital signature generation; and in the second place, it provides a source of cryptographically strong pseudo-random numbers, for the generation of keys and signatures.

However, it can also be used as a stand-alone library. To load this library:

#Include SHA–1.DEF

The file SHA–1.DEF is supplied with the distribution kit, in the `BasicCardPro\Lib` directory.

6.5.1 Hashing Functions

If a message is contained in a **String**, you can compute its hash with a single function call:

Function ShaHash (S\$) As String

To hash longer messages, you must use the following procedures:

Professional BasicCard:

Sub ShaStart (HashBuff\$)

Sub ShaAppend (HashBuff\$, S\$)

Function ShaEnd (HashBuff\$) As String

Other Environments:

Sub ShaStart()

Sub ShaAppend (S\$)

Function ShaEnd() As String

Call **ShaStart()** to initialise the hashing process, then **ShaAppend (S\$)** for successive blocks of data, and finally **ShaEnd()** to get the 20-byte hash value. In the Professional BasicCard, the *HashBuff\$* argument is used to store the internal state of the hash algorithm; other environments have static buffers for this purpose.

6. Plug-In Libraries

6.5.2 Pseudo-Random Number Generation

Only the Professional BasicCard has its own hardware random number generator; other environments must generate pseudo-random numbers in software. The Secure Hash Algorithm is one source of cryptographically strong pseudo-random numbers. To do this properly, it must be fed with some initial source of random data, for instance user key-strokes (see example program **ECTERM** in directory BasicCardPro\Examples\EC).

Sub ShaRandomSeed (Seed\$)

This function mixes the given seed into the 'randomness pool'.

Function ShaRandomHash() As String

This function returns a 20-byte random string. Each byte in the string is a random number between 0 and 255 inclusive.

Each time that you call **ShaRandomSeed (Seed\$)**, the seed is mixed into the 'randomness pool'. The effect is cumulative, so the more data you mix in, the better. The ZC-Basic interpreter mixes in some data of its own each time this procedure is called:

- The Terminal program mixes in the date and time, and the elapsed CPU time for the process.
- The Enhanced BasicCard mixes in its unique serial number. So any two cards will generate different sequences, even if they are fed with the same seeds.

The Enhanced BasicCard has no other internal source of randomness, so you must send it random data from the Terminal program if cryptographically strong random numbers are required, for instance when generating key pairs for use by the **EC-161** Elliptic Curve Cryptography library.

6.6 IDEA: International Data Encryption Algorithm

The **IDEA** library implements the International Data Encryption Algorithm, a block cipher with a 128-bit key size. This algorithm is cryptographically as strong as Triple DES, but is more than three times as fast. To load this library:

#Include IDEA.DEF

The file IDEA.DEF is supplied with the distribution kit, in the BasicCardPro\Lib directory.

Note: The International Data Encryption Algorithm may be used free of charge for non-commercial purposes. For commercial use, permission must be obtained from the patent holders:

Ascom Systec Ltd.	Internet: http://www.ascom.com/infosec
Gewerbepark	e-mail: IDEA@ascom.ch
CH-5506 Maegenwil	
Switzerland	

6.6.1 IDEA Functions

The library provides two functions:

Function IdeaEncrypt (Key\$, Data\$) As String

Function IdeaDecrypt (Key\$, Data\$) As String

Key\$ The 16-byte cryptographic key.

Data\$ The 8-byte data block to be encrypted or decrypted.

Both functions return an 8-byte string.

If **Len(Key\$) < 16** or **Len(Data\$) < 8**, variable **LibError** is set to **IdeaBadProcParams (&H4301)**.

The **IDEA** algorithm can be used in various modes of operation: Electronic Codebook (**ECB**) mode, Cipher Feedback (**CFB**) mode, etc. These modes have been implemented in ZC-Basic in the file IDEATEST.BAS, in the directory BasicCardPro\Examples\IDEA.

6.7 MATH: Mathematical Functions

The **MATH** library provides standard mathematical functions such as **Exp** and **Sin**. It may only be used in Terminal programs. To load this library:

#Include MATH.DEF

The file MATH.DEF is supplied with the distribution kit, in the `BasicCardPro\Lib` directory.

6.7.1 Error Codes

The **MATH** library procedures can signal the following error codes in **LibError**:

MathDomain	A parameter was outside the valid range, e.g. Log (−1.0)
MathSingularity	The function has a singularity at the given point, e.g. Tan (MathPi / 2)
MathOverflow	The maximum Single value of 3.402823E+38 was exceeded
MathUnderflow	The minimum Single value of 1.401298E−45 was truncated to zero
MathLossOfPrecision	Total loss of precision renders the result meaningless, e.g. Sin (1E30)

These constants are defined in MATH.DEF.

6.7.2 Integer Rounding

Function Floor (X!) As Single	The largest integer $\leq X!$, as a Single value
Function Ceil (X!) As Single	The smallest integer $\geq X!$, as a Single value

6.7.3 Exponentiation

Function Pow (X!, Y!) As Single	$X!$ to the power $Y!$
Function Exp (X!) As Single	e to the power $X!$ (e is the base of natural logarithms)
Function LogE (X!) As Single	The natural logarithm of $X!$ (i.e. the logarithm to base e)
Function Log10 (X!) As Single	The logarithm of $X!$ to base 10

6.7.4 Trigonometric Functions

Function Hypot (X!, Y!) As Single	Sqrt ($X! * X! + Y! * Y!$) (with no intermediate overflow)
Function Sin (X!) As Single	Sine function
Function Cos (X!) As Single	Cosine function
Function Tan (X!) As Single	Tangent function Tan (X!) = Sin (X!) / Cos (X!)
Function ASin (X!) As Single	Inverse Sine function ($-\pi/2 \leq \text{ASin} (X!) \leq \pi/2$)
Function ACos (X!) As Single	Inverse Cosine function ($0 \leq \text{ACos} (X!) \leq \pi$)
Function ATan (X!) As Single	Inverse Tangent function ($-\pi/2 < \text{ATan} (X!) < \pi/2$)
Function ATan2 (Y!, X!) As Single	Inverse Tangent at (X!, Y!) ($-\pi < \text{ATan2} (Y!, X!) \leq \pi$)

6.7.5 Hyperbolic Functions

Function SinH (X!) As Single	Hyperbolic Sine: $(\text{Exp} (X!) - \text{Exp} (-X!)) / 2$
Function CosH (X!) As Single	Hyperbolic Cosine: $(\text{Exp} (X!) + \text{Exp} (-X!)) / 2$
Function TanH (X!) As Single	Hyperbolic Tangent: SinH (X!) / CosH (X!)

6.7.6 Mathematical Constants

The following constants are defined in MATH.DEF:

Const MathE = 2.718281828	The base e of natural logarithms
Const MathPi = 3.141592654	π

6. Plug-In Libraries

6.8 MISC: Miscellaneous Procedures

The **MISC** library provides miscellaneous utility procedures. To load this library:

#Include MISC.DEF

The file **MISC.DEF** is supplied with the distribution kit, in the `BasicCardPro\Lib` directory. It contains the following procedures, all of which are defined in more detail below:

For Terminal programs:

<i>Timing Functions</i>	Sub GetDateTime (<i>DT As DateTime</i>) Function TimeInterval (<i>StartTime As DateTime, EndTime As DateTime</i>) As Long Function UnixTime () As Long
<i>Suspending the Program</i>	Sub Sleep (<i>Milliseconds As Long</i>)
<i>Executing a Command Line</i>	Sub Execute (<i>CommandString\$</i>)
<i>CRC Calculations</i>	Function CRC16 (<i>S\$</i>) As Integer Sub UpdateCRC16 (<i>CRC, S\$</i>) Function CRC32 (<i>S\$</i>) As Long Sub UpdateCRC32 (<i>CRC As Long, S\$</i>)
<i>Random String</i>	Sub RandomString (<i>S\$, Len</i>)
<i>Making a Noise</i>	Sub Beep (<i>Frequency, Duration As Long</i>)

For Enhanced BasicCards **ZC3.3**, **ZC3.4**, **ZC3.5**, **ZC3.6**:

<i>Fast EEPROM Writes</i>	Sub FastEepromWrites ()
---------------------------	--------------------------------

For Professional BasicCards:

<i>Random String</i>	Sub RandomString (<i>S\$, Len</i>)
<i>Communications</i>	Function LePresent () Sub SuspendSW1SW2Processing ()

6.8.1 Timing Functions

Three timing procedures are provided, for use in Terminal programs only.

Two of these procedures take parameters of type **DateTime**, defined in **MISC.DEF**:

```
Type DateTime  
  Year, Month, Day  
  Hour, Minute, Second  
  Millisecond  
End Type
```

Sub GetDateTime (*DT As DateTime*)

Returns the current system date and time in *DT*.

Note: *DT* is filled in from the system clock. Under MS-DOS and Windows, the system clock has a resolution of about 55 milliseconds, which is rounded to a multiple of 10. So values returned by **GetDateTime** will jump in increments of 50 or 60 milliseconds.

Function TimeInterval (*StartTime As DateTime, EndTime As DateTime*) **As Long**

Returns the time interval between *StartTime* and *EndTime*, in milliseconds. This interval will be a multiple of the system clock resolution; see note to **GetDateTime**.

For examples of the use of these procedures, see programs **ECINIT.BAS** and **ECTEST.BAS** in directory `BasicCardPro\Examples\EC`.

The third timing procedure returns the number of seconds elapsed since 1st January 1970:

Function UnixTime() **As Long**

6.8.2 *Suspending the Program*

In a Terminal program, the following subroutine suspends execution for the specified number of milliseconds:

Sub Sleep (*Milliseconds As Long*)

This frees the CPU for other processes to use.

6.8.3 *Executing a Command Line*

An operating system command can be executed from a Terminal program using the **Execute** subroutine:

Sub Execute (*CommandString\$*)

The following error codes are returned in the **LibError** variable:

MiscCommandTooLong	Under MS-DOS, the command string was longer than 128 bytes
MiscFileNotFound	The command string specified a non-existent executable file
MiscNotExecutable	The command string specified a non-executable file
MiscOutOfMemory	Insufficient memory to execute the command
MiscUnexpectedError	The operating system returned an unexpected error code

These constants are defined in MISC.DEF.

Note that it is not possible to retrieve an error code generated by the command itself.

6.8.4 *CRC Calculations*

Function CRC16 (<i>S\$</i>) As Integer	Returns the 16-bit CRC of the string <i>S\$</i>
Sub UpdateCRC16 (<i>CRC, S\$</i>)	Allows cumulative calculation of 16-bit CRC's
Function CRC32 (<i>S\$</i>) As Long	Returns the 32-bit CRC of the string <i>S\$</i>
Sub UpdateCRC32 (<i>CRC As Long, S\$</i>)	Allows cumulative calculation of 32-bit CRC's

To calculate the CRC of a single **String** value, call **CRC16** or **CRC32**. To calculate CRC's for larger amounts of data, first initialise *CRC* to zero, then call **UpdateCRC16** or **UpdateCRC32** with successive values of *S\$*.

Here are 'C' functions to calculate the 16-bit and 32-bit CRC's:

```

unsigned short CRC (unsigned char *p, unsigned int len)
{
    unsigned short crc = 0 ;
    while (len--)
    {
        unsigned char NextByte = *p++ ;
        int i ;
        for (i = 0 ; i < 8 ; i++, NextByte >>= 1)
        {
            if ((crc ^ NextByte) & 1)
            {
                crc >>= 1 ;
                crc ^= 0xCA00 ;
            }
            else crc >>= 1 ;
        }
    }
    return crc ;
}

```


6. Plug-In Libraries

```
unsigned long CRC32 (unsigned char *p, unsigned int len)
{
    unsigned long crc = 0 ;
    while (len--)
    {
        unsigned char NextByte = *p++ ;
        int i ;
        for (i = 0 ; i < 8 ; i++, NextByte >>= 1)
        {
            if ((crc ^ NextByte) & 1)
            {
                crc >>= 1 ;
                crc ^= 0xA3000000 ;
            }
            else crc >>= 1 ;
        }
    }
    return crc ;
}
```

6.8.5 Making a Noise

The Terminal program can generate an audible beep with the **Beep** subroutine:

Sub Beep (*Frequency, Duration As Long*)

The duration is in milliseconds.

Note: The *Frequency* and *Duration* parameters are only effective under Windows NT and Windows 2000; they are ignored under Windows 98 (although they must be present).

6.8.6 Fast EEPROM Writes

The EEPROM in the Enhanced BasicCard has an erase/write cycle time of 6 milliseconds – it takes this long to guarantee that each bit has been completely discharged and/or recharged. The BasicCard has no internal clock, so it must count instruction cycles to estimate the elapsed time. However, it has no way of knowing the clock frequency, so it must assume the worst case – it must assume that the clock is running at its maximum allowed speed. This maximum speed is specified in standard ISO/IEC 7816-3 as 5 MHz.

If the card reader is generating a slower clock frequency, then EEPROM writes will take longer than they need to. For instance, most readers (including ZeitControl's Chipi and CyberMouse card reader) generate a clock frequency of 3.57 MHz; so instead of 6 milliseconds, an EEPROM write takes 8.4 milliseconds. If speed is important to you, and if you know that the clock frequency is only 3.57 MHz (or less), you can call the following procedure:

Sub FastEepromWrites()

The BasicCard operating system will then speed up its EEPROM writes, so that they take 6 milliseconds at the assumed slower clock speed. This procedure is available for Enhanced BasicCards **ZC3.3**, **ZC3.4**, **ZC3.5**, and **ZC3.6**.

Warning: If in fact the card reader is running at faster than 3.57 MHz, calling this procedure may result in subsequent loss of EEPROM data through charge leakage.

6.8.7 Random String

In the Terminal program and in all current Professional BasicCards, a **String** variable can be filled with random data:

Sub RandomString (*S\$, Len*)

On return, *S\$* contains *Len* bytes of random data.

6.8.8 *SW1-SW2 Processing*

Normally, if **SW1-SW2** \neq **&H9000**, and **SW1** \neq **&H61**, then **ODATA** is not sent – see **7.5 Commands and Responses**. You can override this behaviour in some Professional BasicCards with the following procedure call:

Sub SuspendSW1SW2Processing()

The card will then send the **ODATA** field in the response, regardless of the value of **SW1-SW2**. This procedure only affects the current command. See **3.3.3 Options** for an alternative method.

At the time of writing, this procedure is available in Professional BasicCards **ZC4.5A** (from Revision D), **ZC4.5D** (from Revision D), and **ZC5.5** (all revisions).

Part II

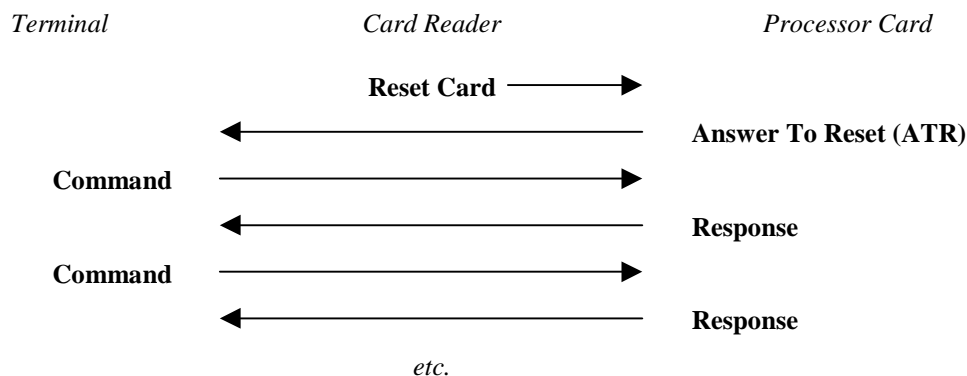
Technical Reference

7. Communications

Note: Throughout this chapter, **bold** numbers are hexadecimal.

7.1 Overview

As outlined in **1.1 Processor Cards**, communication between a Terminal and a Processor Card proceeds, via a Card Reader, as a series of Commands (initiated by the Terminal) and Responses (sent by the Processor Card). The series starts with the Card Reader sending a **Reset Card** signal to the Processor Card:



Two documents describe this process in detail:

1. **ISO/IEC 7816-3:** *Electronic signals and transmission protocols*

This document describes the communication between the Card Reader and the Processor Card, from the bit level through the byte level to the block level. We will be concerned with three aspects:

- the structure of the **ATR**;
- the **T=0** character transmission protocol;
- the **T=1** block transmission protocol.

2. **ISO/IEC 7816-4:** *Interindustry commands for interchange*

This document describes Commands and Responses. We will be concerned with three aspects:

- the contents of Commands and Responses;
- the method by which the **T=0** protocol transmits Commands and Responses;
- the method by which the **T=1** protocol transmits Commands and Responses.

We provide a summary of these documents in the following sections. Most readers can skip these sections; they are provided mainly for users who need to program the BasicCard to be compatible with existing systems.

In these documents, a Command or Response is referred to as an **APDU** (application protocol data unit). The structure of Command and Response **APDU**'s is described in **7.5 Commands and Responses**.

7.2 Answer To Reset

With the Answer To Reset (**ATR**), the Processor Card identifies itself and indicates which protocols it supports. Most of the data in the **ATR** is not relevant to a BasicCard programmer. The following information is important:

- whether the card supports the **T=0** and/or the **T=1** protocols;
- the maximum communication speed that the card allows;
- the Historical Characters.

The Compact and Enhanced BasicCards support only the **T=1** protocol, at 9600 baud. They send the following **ATR** (the byte names are from ISO/IEC):

TS	T0	TB1	TC1	TD1	TD2	TA3	TB3	T1-TK
3B	EF	00	FF	81	31	50 or 20	45 or 75	'BasicCard ZC _{vvv} '

Briefly, what this means is:

TS = 3B	Direct convention (high = 1 , low = 0 ; least significant bit arrives first)
T0 = EF	E → TB1 , TC1 , TD1 follow; F → 15 historical characters
TB1 = 00	No EEPROM programming voltage required
TC1 = FF	Waiting time between two characters = 11 ETU
TD1 = 81	TD2 follows (T=1 indication)
TD2 = 31	TA3 , TB3 follow (T=1 indication)
TA3 = 50 or 20	IFSC (Information Field Size) = &H50 in Compact card, &H20 in Enhanced card
TB3 = 45 or 75	CWT (character waiting time) = (11 + 32) ETU (= 3.33 ms between characters) In ZC1.1, ZC3.3, and ZC3.5 cards (TB3 = 45): BWT (block waiting time) = (11 + 16*960) ETU (= 1.6 seconds between blocks) In later cards (TB3 = 75): BWT (block waiting time) = (11 + 128*960) ETU (= 12.8 seconds between blocks)
T1-TK	The historical characters (_{vvv} is the BasicCard firmware version number)

An **ETU** (elementary time unit) is one bit, or 372 clock cycles. The timing figures assume a clock frequency of 3.57 MHz. Historical characters **T1-TK** can be configured in ZC-Basic with the **Declare ATR** statement; the whole of the **ATR** can be specified with **Declare Binary ATR** – see **3.20.1 Customised ATR**.

The Professional BasicCards are more flexible in their capabilities; they support the **T=0** protocol as well as the **T=1** protocol, and they can run at up to 38400 baud. Here is a typical **ATR** (from the Professional BasicCard “**ZC4.5D REV C**”):

TS	T0	TA1	TB1	TC1	TD1	TC2	T1-TK
3B	FC	13	00	FF	40	80	'ZC4.5D REV C'

TS = 3B	Direct convention (high = 1 , low = 0 ; most significant bit arrives first)
T0 = FC	F → TA1 , TB1 , TC1 , TD1 follow; C → 12 historical characters
TA1 = 13	FI = 1 ; DI = 3 → maximum allowed communication speed = 38400 baud
TB1 = 00	No EEPROM programming voltage required
TC1 = FF	Waiting time between two characters = 11 ETU
TD1 = 40	TC2 follows (T=0 indication)
TC2 = 80	WWT (work waiting time) = 12.8 seconds

7.3 The T=0 Protocol

The **T=0** protocol is a character-level transmission protocol for integrated circuit cards with contacts, defined in the document **ISO/IEC 7816-3: Electronic signals and transmission protocols**. Some Professional BasicCards support the **T=0** protocol, as well as the **T=1** protocol described in the next section. **T=1** is faster, easier to use, and less error-prone; you should only use the **T=0** protocol if you are implementing a pre-existing **T=0** command set, or you need to use card readers that don't support the **T=1** protocol.

The **T=0** protocol is defined as a sequence of messages exchanged between the **IFD** (interface device) and the **ICC** (integrated circuit card). In the present context, the **IFD** is the Terminal program, and the **ICC** is the BasicCard. The exchange begins when the **ICC** is powered up and responds with an **ATR** (Answer To Reset). Thereafter the **IFD** sends a **TPDU** (transmission protocol data unit) containing a

7. Communications

Command, and the **ICC** replies with a **TPDU** containing the Response. A **TPDU** is a lower-level object than an **APDU**; we will see later how **APDU**'s are constructed from **TPDU**'s.

7.3.1 TPDU Transmission

When the **IFD** sends a Command **TPDU** and the **ICC** replies with a response **TPDU**, only one of the two **TPDU**'s may contain data. If the Command **TPDU** contains data, it is an *incoming data transfer*; if the Response **TPDU** contains data, it is an *outgoing data transfer*. The **T=0** protocol does not provide any mechanism for specifying which of the two **TPDU**'s may contain data; and in fact the protocol grinds to a halt if the **IFD** and **ICC** don't agree on the direction of data transfer.

In both cases, the **IFD** first sends a 5-byte command header:

CLA	INS	P1	P2	P3
-----	-----	----	----	----

- CLA** Class byte – first byte of two-byte **CLA INS** command identifier. This byte may not be **FF**.
- INS** Instruction byte – second byte of two-byte **CLA INS** command identifier. **INS** must be even, and the top nibble may not be **6** or **9**.
- P1** Parameter 1 of 4-byte **CLA INS P1 P2** command header.
- P2** Parameter 2 of 4-byte **CLA INS P1 P2** command header.
- P3** Number of data bytes.

From the command header, the **ICC** must be able to determine whether the **IFD** expects an incoming or outgoing data transfer.

Incoming Data Transfer

Command TPDU:	CLA	INS	P1	P2	P3	D ₁	...	D _{P3}
---------------	-----	-----	----	----	----	----------------	-----	-----------------

Response TPDU:	SW1	SW2
----------------	-----	-----

The **ICC** acknowledges the 5-byte command header by echoing the **INS** byte (more variations are described in the **ISO/IEC** document, but the BasicCard does not use them):

←	INS
---	-----

The **IFD** then sends **P3** bytes of data:

D ₁	...	D _{P3}
----------------	-----	-----------------

The **ICC** responds with a two-byte status code:

←	SW1	SW2
---	-----	-----

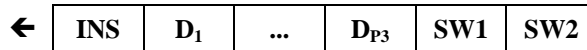
where the top nibble of **SW1** is **6** or **9** (but **SW1=60** is not allowed). Status codes are described in **7.6 Status Bytes SW1 and SW2**.

Outgoing Data Transfer

Command TPDU:	CLA	INS	P1	P2	P3
---------------	-----	-----	----	----	----

Response TPDU:	D ₁	...	D _{P3}	SW1	SW2
----------------	----------------	-----	-----------------	-----	-----

The **ICC** acknowledges the 5-byte command header by echoing the **INS** byte, and then sends **P3** data bytes, followed by a two-byte status code:



In both cases, the **ICC** may reject the command by responding immediately with **SW1-SW2** instead of echoing **INS**.

If the **WWT** work waiting time is exceeded, the **IFD** will time out. The **ICC** can restart the timer, and so delay the time out, by sending a **NULL (60)** byte. In a BasicCard program, this is done with the **WTX** statement:

WTX *n*

The ZC-Basic syntax requires the parameter *n*, although it is ignored if the card is using **T=0** protocol.

7.3.2 APDU Transmission by T=0

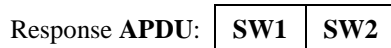
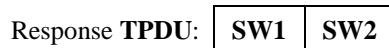
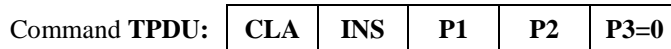
This section describes the methods defined by ISO/IEC for implementing **APDU** exchanges under **T=0**. If you are not familiar with the structure of Command and Response **APDU**'s, you should read **7.5 Commands and Responses** before continuing.

There are four cases to consider. We adhere to the notation in **ISO/IEC 7816-4: Interindustry commands for interchange, Annex A** (normative): **Transportation of APDU messages by T=0**:

- Case 1:** **Lc=0**, and **Le** not present: no incoming data, and no outgoing data
- Case 2:** **Lc=0**, and **Le** present: outgoing data only
- Case 3:** **Lc** non-zero, and **Le** not present: incoming data only
- Case 4:** **Lc** non-zero, and **Le** present: incoming and outgoing data

7.3.3 Case 1: No Incoming Data or Outgoing Data

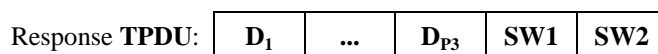
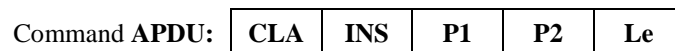
The Command **TPDU** consists of the Command **APDU** with **P3=0** appended:



7.3.4 Case 2: Outgoing Data Only

Case 2S.1 – Le accepted

If the **ICC** accepts the value of **Le** supplied by the **IFD**, the Command and Response **TPDU** are identical to the Command and Response **APDU**:



7. Communications

Case 2S.2 – Le definitely not accepted

If the ICC does not accept **Le**, and does not want to suggest an alternative, it replies with **SW1-SW2=6700**:

Command **APDU**:

CLA	INS	P1	P2	Le
------------	------------	-----------	-----------	-----------

Command **TPDU**:

CLA	INS	P1	P2	P3=Le
------------	------------	-----------	-----------	--------------

Response **TPDU**:

67	00
-----------	-----------

Response **APDU**:

67	00
-----------	-----------

Case 2S.3 – Le not accepted, La indicated

If the ICC does not accept **Le**, and has an alternative **La** to suggest, it responds with **SW1-SW2 = 6C La**, and the **IFD** can re-issue the command to receive the outgoing data:

Command **APDU**:

CLA	INS	P1	P2	Le
------------	------------	-----------	-----------	-----------

Command **TPDU**:

CLA	INS	P1	P2	P3=Le
------------	------------	-----------	-----------	--------------

Response **TPDU**:

6C	La
-----------	-----------

Command **TPDU**:

CLA	INS	P1	P2	P3=La
------------	------------	-----------	-----------	--------------

Response **TPDU**:

D₁	...	D_{La}	SW1	SW2
----------------------	------------	-----------------------	------------	------------

Response **APDU**:

D₁	...	D_{La}	61	La
----------------------	------------	-----------------------	-----------	-----------

Case 2S.4 – Command not accepted

Command **APDU**:

CLA	INS	P1	P2	Le
------------	------------	-----------	-----------	-----------

Command **TPDU**:

CLA	INS	P1	P2	P3=Le
------------	------------	-----------	-----------	--------------

Response **TPDU**:

SW1	SW2
------------	------------

Response **APDU**:

SW1	SW2
------------	------------

with **SW1=6X** except **6C**, or **SW1-SW2=9XXX** except **9000**.

7.3.5 Case 3: Incoming Data Only

The Command and Response **TPDU** are identical to the Command and Response **APDU**:

Command **APDU**:

CLA	INS	P1	P2	Lc	D₁	...	D_{Lc}
------------	------------	-----------	-----------	-----------	----------------------	-----	-----------------------

Command **TPDU**:

CLA	INS	P1	P2	P3=Lc	D₁	...	D_{P3}
------------	------------	-----------	-----------	--------------	----------------------	-----	-----------------------

Response **TPDU**:

SW1	SW2
------------	------------

Response **APDU**:

SW1	SW2
------------	------------

7.3.6 Case 4: Incoming and Outgoing Data

The Command **TPDU** is identical to the Command **APDU**, but with **Lc** removed:

Command **APDU**:

CLA	INS	P1	P2	Lc	D₁	...	D_{Lc}	Le
------------	------------	-----------	-----------	-----------	----------------------	-----	-----------------------	-----------

Command **TPDU**:

CLA	INS	P1	P2	P3=Lc	D₁	...	D_{P3}
------------	------------	-----------	-----------	--------------	----------------------	-----	-----------------------

Depending on the response, the **IFD** may issue a **GET RESPONSE** Command to request the outgoing data. This command has **INS=C0**, **P1=0**, **P2=0**, but the ISO/IEC document leaves the **CLA** byte unspecified. ZeitControl's Terminal software (the **IFC**) uses **CLA=0**; the BasicCard operating system accepts any value for **CLA** that is not a user-defined command.

Case 4S.1 – Command not accepted

Response **TPDU**:

SW1	SW2
------------	------------

Response **APDU**:

SW1	SW2
------------	------------

with **SW1=6X** except **61**, or **SW1-SW2=9XXX** except **9000**.

Case 4S.2 – Command accepted

Response **TPDU**:

90	00
-----------	-----------

The **IFD** issues a **GET RESPONSE** Command:

Command **TPDU**:

CLA=00	INS=C0	P1=00	P2=00	P3=Le
---------------	---------------	--------------	--------------	--------------

Transmission then proceeds as in *Case 2*.

Case 4S.3 – Command accepted with information added

The **ICC** accepts the command, and indicates that **Lx** bytes of outgoing data are available:

Response **TPDU**:

61	Lx
-----------	-----------

The **IFD** issues a **GET RESPONSE** Command, with **P3=min(Le,Lx)**:

Command **TPDU**:

CLA=00	INS=C0	P1=00	P2=00	P3
---------------	---------------	--------------	--------------	-----------

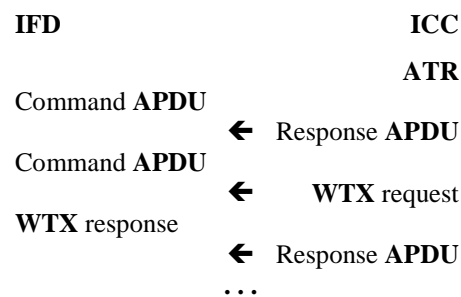
Transmission then proceeds as in *Case 2*.

7.4 The T=1 Protocol

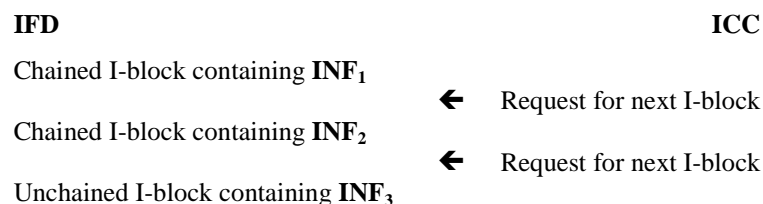
The **T=1** protocol is a block-level transmission protocol for integrated circuit cards with contacts, defined in the document **ISO/IEC 7816-3: Electronic signals and transmission protocols**. The BasicCard contains a full implementation of this **T=1** standard, including **NAD** awareness, chaining, retries, **WTX** requests, and **IFS** requests. This section describes those parts of the **T=1** protocol that a programmer of the BasicCard might want to know: (i) the error-free transmission of I-blocks; (ii) the **WTX** request. The mechanisms for chaining, error handling, and **IFS** adjustment are hidden from the programmer, and are not described here. For a detailed definition of the **T=1** protocol, see document **ISO/IEC 7816-3**.

7.4.1 APDU Transmission by T=1

The **T=1** protocol is defined as a sequence of messages exchanged between the **IFD** (interface device) and the **ICC** (integrated circuit card). In the present context, the **IFD** is the Terminal program, and the **ICC** is the BasicCard. The exchange begins when the **ICC** is powered up and responds with an **ATR** (Answer To Reset). Thereafter the **IFD** sends an **APDU** containing a Command, and the **ICC** replies with an **APDU** containing the Response. In between receiving a command and sending its response, the **ICC** may transmit a **WTX** request (waiting time extension), to ask for more time:



Each **APDU** is transmitted in one or more *I-blocks*. An I-block is the fundamental unit of transmission in the **T=1** protocol; successive I-blocks are chained together to produce the Command and Response **APDU**'s. In the following example, **APDU** is the concatenation of **INF₁**, **INF₂**, and **INF₃**:



The maximum allowed length of an I-block depends on the direction of transmission, and on protocol parameters that can vary dynamically; it is typically 32-128 bytes.

7.4.2 Structure of an I-block

An I-block contains the following fields. All fields are one byte, except the **INF**:



NAD Node Address byte. The low nibble contains the Node Address (0-7) of the sender, and the high nibble contains the Node Address (0-7) of the intended recipient. The BasicCard responds to all Node Address values, unless otherwise instructed with the pre-defined **ASSIGN NAD** command. The **NAD** of the response I-block is equal to the **NAD** of the command I-block with the high and low nibbles reversed.

PCB Protocol control byte. Alternates between **00** and **40** (unless chaining is in progress). The BasicCard programmer can ignore this byte.

LEN	The length of the INF field in bytes.
INF	Information field – the information content of the I-block. The T=1 protocol says nothing about the internal format of the INF field.
LRC	Longitudinal redundancy check. A simple Xor of all the preceding bytes.

7.4.3 WTX Request

The **BWT** (block waiting time) defined in the **ATR** tells the **IFD** how long to wait for a response before timing out. The BasicCard **ATR** defines a **BWT** of 1.6 seconds (BasicCard versions ZC1.1, ZC3.3, and ZC3.5), or 12.8 seconds (all other BasicCards). If a command is going to take longer than this, it must request more time using a **WTX** (waiting time extension) request. In ZC-Basic, this takes the form

WTX BWT-units

BWT-units A **Byte** expression, giving the requested time in multiples of the **BWT**. **WTX** requests are not cumulative; the time allowed is counted from the time of the request, and cancels any previous **WTX** requests.

A **WTX** request contains the following fields:

WTX request:	NAD	PCB=C3	LEN=01	INF	LRC
---------------------	------------	---------------	---------------	------------	------------

The **INF** field has length 1, and contains the value *BWT-units*. The response to this request contains an identical **INF** field:

WTX response:	NAD	PCB=E3	LEN=01	INF	LRC
----------------------	------------	---------------	---------------	------------	------------

7.5 Commands and Responses

This section describes the contents of commands and responses, as defined in the document **ISO/IEC 7816-4: Interindustry commands for interchange**. The **APDU** of a command has the following structure (shaded blocks are optional):

CLA	INS	P1	P2	Lc	IDATA	Le
------------	------------	-----------	-----------	-----------	--------------	-----------

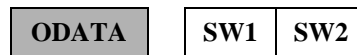
CLA	Class byte – first byte of two-byte CLA INS command identifier. If the T=0 protocol is used, this byte may not be FF .
INS	Instruction byte – second byte of two-byte CLA INS command identifier. For ISO compatibility, this byte should be even. If the T=0 protocol is used, the top nibble may not be 6 or 9 .
P1	Parameter 1 of 4-byte CLA INS P1 P2 command header.
P2	Parameter 2 of 4-byte CLA INS P1 P2 command header.
Lc	Length of IDATA field in command.
IDATA	Data expected by command. In the case of a ZC-Basic command, this field contains the parameters passed by the caller.
Le	Expected length of ODATA field in response (supplied by caller).

In the BasicCard, **CLA** and **INS** can refer to pre-defined commands (all of which have **CLA=C0**) or ZC-Basic commands (**CLA** and **INS** are specified by the programmer for each command). **P1** and **P2** are retained in the BasicCard for **ISO** compatibility; you can use them if you like, or ignore them. If you want to use them, the parameters passed to you by the caller are available as **Public Byte** variables **P1** and **P2**; and you can specify their values in commands that you call using the *PreSpec* field described in **3.14.3 Calling a Command**:

Call *command-name* ([**P1=expr**,] [**P2=expr**,] *arg-list*)

7. Communications

The **APDU** of a response has the following structure (the shaded block is optional):



ODATA Data returned by command. In the case of a ZC-Basic command, this field contains the parameters that were passed by the caller, as modified by the called command.

SW1 First status byte.

SW2 Second status byte.

SW1 and **SW2** are pre-defined **Public** variables of type **Byte**. Before a command is executed, they have the values **&H90** and **&H00**, which is a standard status code meaning “Command successfully completed”. If you want to return an error code to the caller, just set **SW1** and **SW2** to the appropriate values before you exit the command.

Notes:

- if **SW1-SW2** \neq **&H9000**, and **SW1** \neq **&H61**, then **ODATA** is discarded: any return values are lost. In some Professional BasicCards, you can override this behaviour – see **3.3.3 Options** and **6.8.8 SW1-SW2 Processing**.
- in a card using the **T=0** protocol, the high nibble of **SW1** must be **6** or **9**.

7.6 Status Bytes SW1 and SW2

7.6.1 BasicCard Operating System

The following status codes are returned by the BasicCard operating system:

swCommandOK	9000	Command successfully completed.
sw1LeWarning	61XX	Command successfully completed, but Le was not equal to XX .
swRetriesRemaining	63CX	A command was wrongly encrypted, and the error counter for the active key has been decremented to X . If X reaches zero, the key is disabled.
sw1PCodeError	64XX	P-Code error XX occurred in the BasicCard. (The P-Code error codes are described in the next section.)
swEepromWriteError	6581	A write to EEPROM failed. (This is a hardware error.)
swBadEepromHeap	6582	The EEPROM heap is in an inconsistent state.
swBadFileChain	6583	The BasicCard File System is in an inconsistent state.
swKeyNotFound	6611	The key specified in a START ENCRYPTION command was not configured with a Declare Key statement in the BasicCard program.
swPolyNotFound	6612	The SG-LFSR algorithm was specified in a START ENCRYPTION command, but primitive polynomials were not configured with a Declare Polynomials statement in the BasicCard program.
swKeyTooShort	6613	The cryptographic key specified in a START ENCRYPTION command was too short for the algorithm. All algorithms require at least 8-byte keys; the Triple DES algorithm requires 16-byte keys.
swKeyDisabled	6614	The active key has been disabled, either explicitly with a Disable Key statement, or automatically when its error counter reached zero.
swUnknownAlgorithm	6615	Parameter P1 in a START ENCRYPTION command does not specify a valid algorithm.

swAlreadyEncrypting	66C0	A START ENCRYPTION command was received while encryption was already active.
swNotEncrypting	66C1	An END ENCRYPTION command was received while encryption was not active.
swBadCommandCRC	66C2	The active encryption algorithm is SG_LFSR with CRC , and the CRC in a command was invalid.
swDesCheckError	66C3	The active encryption algorithm is Single DES or Triple DES , and the authentication bytes in a command were invalid.
swCoprocesorError	66C4	The Crypto-Coprocessor has reported an internal error.
swAesCheckError	66C5	The active encryption algorithm is AES , and the authentication bytes in a command were invalid.
swLcLeError	6700	Either Lc has an unexpected value; or Le is absent when it should be present, or present when it should be absent.
swCommandTooLong	6781	A command will not fit in the command buffer. In the Compact BasicCard, this is the same size as the P-Code stack; in the Enhanced BasicCard, it is 256 bytes. (In state LOAD , other limits may apply, but the software support package handles this case.)
swResponseTooLong	6782	The response from the card is too long to be sent.
swInvalidState	6985	A built-in command was called, but the state of the BasicCard is invalid for the command.
swCardUnconfigured	6986	The card has not been configured by ZeitControl.
swNewStateError	6987	The state of the BasicCard has been changed with a SET STATE command. After a SET STATE command, the BasicCard must be reset before it will accept any further commands.
swP1P2Error	6A00	P1 or P2 is invalid for the command.
swOutsideEeprom	6A02	An invalid address was passed in PIP2 to one of the built-in EEPROM access commands.
swDataNotFound	6A88	The built-in command GET APPLICATION ID returns this error code if no Application ID was configured in the BasicCard.
sw1LaWarning	6CXX	Command successfully completed, but La was not equal to XX .
swINSNotFound	6D00	The INS byte of the command was not recognised (although the CLA byte was valid).
swCLANotFound	6E00	The CLA byte of the command was not recognised.
swInternalError	6F00	An unexpected error condition was detected.

7.6.2 BasicCard P-Code Interpreter

If the P-Code interpreter in the BasicCard detects an error, it returns **sw1PCodeError (64)** in **SW1**, and the specific P-Code error in **SW2**. The P-Code error is one of the following:

pcStackOverflow	01	The P-Code stack has grown beyond its configured size.
pcDivideByZero	02	A division by zero (or a Mod with zero divisor) occurred.
pcNotImplemented	03	An unimplemented P-Code instruction was executed (e.g. a floating-point instruction in the Compact BasicCard).
pcBadRamHeap	04	Corruption of RAM has left the heap in an inconsistent state.
pcBadEepromHeap	05	Corruption of EEPROM has left the heap in an inconsistent state.
pcReturnWithoutGoSub	06	A Return statement was executed with no corresponding GoSub.

7. Communications

pcBadSubscript	07	One of the subscripts in an array access was out of bounds.
pcBadBounds	08	One of the array subscript bounds in a ReDim statement was out of range.
pcInvalidReal	09	A floating-point operand was not a valid IEEE-format number.
pcOverflow	0A	The result of an arithmetic operation was too large or small for the destination.
pcNegativeSqrt	0B	An attempt was made to take the square root of a negative number.
pcDimensionError	0C	An array parameter did not have the expected number of dimensions.
pcBadStringCall	0D	An invalid parameter was passed to a string function.
pcOutOfMemory	0E	There was not enough free memory left to complete the instruction.
pcArrayNotDynamic	0F	The array parameter in a ReDim statement was not Dynamic.
pcArrayTooBig	10	The array size requested in a ReDim statement was too large.
pcDeletedArray	11	An attempt was made to access an element of a deleted array.
pcPCodeDisabled	12	A previous P-Code error has disabled the BasicCard. The card must be reset before it can execute P-Code again.
pcBadSystemCall	13	A SYSTEM instruction had an invalid sub-function code.
pcBadKey	14	An invalid key number was passed to a cryptographic function.
pcBadLibraryCall	15	An invalid Plug-In Library function was called.
pcStackUnderflow	16	The P-Code stack has shrunk to a negative size.

7.6.3 Terminal P-Code Interpreter

The P-Code interpreter in the Terminal program can return the following status codes in **SW1-SW2**:

swNoCardReader	6790	No card reader detected on the given COM port.
swCardReaderError	6791	An invalid reply was received to a card reader command.
swNoCardInReader	6792	No card is inserted in the card reader.
swCardPulled	6793	The card has been removed from the card reader.
swT1Error	6794	An unrecoverable T=1 protocol error occurred while communicating with the card.
swCardError	6795	An invalid response was received to a BasicCard command.
swCardNotReset	6796	The card has not been reset. A BasicCard must be reset before the Terminal program can send it any commands.
swKeyNotLoaded	6797	The key specified in a START ENCRYPTION command is unknown to the Terminal program.
swPolyNotLoaded	6798	The SG-LFSR algorithm was specified in a START ENCRYPTION command, but primitive polynomials have not been configured in the Terminal program.
swBadResponseCRC	6799	The active encryption algorithm is SG_LFSR with CRC , and the CRC in a response was invalid.
swCardTimedOut	679A	The card did not respond within the time allowed.
swTermOutOfMemory	679B	The Terminal program has insufficient free memory to process the response.

swBadDesResponse	679C	The active encryption algorithm is Single DES or Triple DES , and the authentication bytes in a response were invalid.
swInvalidComPort	679D	The COM port is not in the range 1-4.
swNoPcscDriver	679F	No PC/SC driver is installed on the PC.
swPcscReaderBusy	67A0	The PC/SC reader is busy.
swPcscError	67A1	An unexpected PC/SC error occurred.
swComPortBusy	67A2	Another process is using the COM port.
swBadATR	67A3	The BasicCard returned an invalid ATR .
swT0Error	67A4	A T=0 protocol error occurred.
swPTSError	67A7	An error occurred during Protocol Type Selection.
swDataOverrun	67A8	The Terminal has lost characters sent by the card reader.
swBadAesResponse	67A9	The active encryption algorithm is AES , and the authentication bytes in a response were invalid.
swReservedINS	6D80	An attempt was made to send a forbidden INS in T=0 protocol.
swReservedCLA	6E80	An attempt was made to send CLA=FF in T=0 protocol.

7.7 Pre-Defined Commands

7.7.1 States of the BasicCard

The Compact and Enhanced BasicCards have four states:

- NEW:** The card is in state **NEW** before ZeitControl configures it.
- LOAD:** The card is in state **LOAD** when the application developer gets it.
- TEST:** State **TEST** lets the application developer test software in the card.
- RUN:** The card is in state **RUN** when it is issued to the end user.

The Professional BasicCard has five states:

- NEW:** The card is in state **NEW** before ZeitControl configures it.
- LOAD:** The card is in state **LOAD** when the application developer gets it.
- PERS:** State **PERS** is for initialising user data.
- TEST:** State **TEST** lets the application developer test software in the card.
- RUN:** The card is in state **RUN** when it is issued to the end user.

The card can be switched between **LOAD**, **PERS**, and **TEST** any number of times, but the **RUN** state is permanent. Once the card is switched to state **RUN**, it can't be re-programmed.

7. Communications

7.7.2 Pre-Defined Commands – a Summary

The BasicCard operating system contains twelve or thirteen pre-defined commands. All commands have class byte **CLA = C0**. The **INS** byte takes the values **00, 02, 04, . . . , 16, 18**, as follows:

GET STATE	00	Get the state and version of the card
EEPROM SIZE	02	Get the address and length of EEPROM
CLEAR EEPROM	04	Set specified bytes to FF
WRITE EEPROM	06	Load data into EEPROM
READ EEPROM	08	Read data from EEPROM
EEPROM CRC	0A	Calculate CRC over a specified EEPROM address range
SET STATE	0C	Set the state of the card
GET APPLICATION ID	0E	Get the Application ID string
START ENCRYPTION	10	Start automatic encryption of command/response data
END ENCRYPTION	12	End automatic encryption
ECHO	14	Echo the command data
ASSIGN NAD	16	Assign a Node Address to the card
FILE IO	18	Execute a file system operation

Most of these commands are enabled only when the BasicCard is in an appropriate state. The following table summarises which internal commands are valid in which states:

	NEW	LOAD	PERS	TEST	RUN
GET STATE	✓	✓	✓	✓	✓
EEPROM SIZE	✓	✓			
CLEAR EEPROM	✓	✓			
WRITE EEPROM	✓	✓			
READ EEPROM	✓	✓	*	*	*
EEPROM CRC	✓	✓			
SET STATE	✓	✓	✓	✓	
GET APPLICATION ID				✓	✓
START ENCRYPTION				✓	✓
END ENCRYPTION				✓	✓
ECHO	✓	✓	✓	✓	✓
ASSIGN NAD	✓	✓	✓	✓	✓
FILE IO		**	✓	✓	✓

* The **READ EEPROM** command is allowed in states **PERS**, **TEST**, and **RUN** if encryption with key number **0** is enabled (see **7.7.6 The READ EEPROM Command**).

** The **FILE IO** command is allowed in state **LOAD** in the Enhanced BasicCard, but not in the Professional BasicCard.

In state **NEW**, no checks are performed on addresses of EEPROM reads and writes. (This is to allow ZeitControl to install upgrades to the BasicCard operating system, before delivery to the application developer.)

In state **LOAD**, the EEPROM access commands are restricted to user EEPROM.

7.7 Pre-Defined Commands

These commands will typically be called at the following points in the development cycle:

1. Write and test a ZC-Basic application on the PC
2. **EEPROM SIZE** – check that the card has the expected EEPROM size
3. **CLEAR EEPROM** – set EEPROM to a known state
4. **WRITE EEPROM** – download the application to the card
5. **EEPROM CRC** – check that the EEPROM was correctly written
6. **FILE IO** – create files and directories
7. **SET STATE** to **TEST** and reset the card
8. Run the application in the card
9. **SET STATE** to **LOAD** and reset the card
10. **READ EEPROM** to check any EEPROM changes made by the application

(Most of this is handled automatically by the ZeitControl MultiDebugger development software.)
When the application is written and tested, cards can be switched into the **RUN** state for delivery to end users.

7. Communications

7.7.3 The GET STATE Command

GET STATE – Get the state and version of the card

Command syntax:

CLA	INS	P1	P2	Le
C0	00	00	00	00

Response:

ODATA	SW1	SW2
state (1 byte), version (n bytes)	61	n+1

This command returns the state and version of the BasicCard.

The *state* byte (Compact and Enhanced BasicCards):

state:	00	01	02	03
State of card:	NEW	LOAD	TEST	RUN

The *state* byte (Professional BasicCards):

state:	00	01	02	03	04
State of card:	NEW	LOAD	PERS	TEST	RUN

The length of the *version* field depends on the card type, as follows:

Compact BasicCard: n = 0 (i.e. no version field is returned)

Enhanced BasicCard: n = 2: major version number (03) followed by minor version number

Professional BasicCard: n >= 3: the version info is an ASCII string

Command-Specific Error Codes in SW1-SW2:

swLcLeError **Lc** is present, or **Le** is absent
swP1P2Error **P1** <> 00 or **P2** <> 00

To call **GET STATE** from a Terminal program:

```
#Include COMMANDS.DEF
Call GetState (State@, Version$)
```


*The EEPROM SIZE Command***EEPROM SIZE** – Get the address and length of EEPROM

Command syntax:

CLA	INS	P1	P2	Le
C0	02	00	00	04

Response:

ODATA	SW1	SW2
<i>start</i> (2 bytes), <i>length</i> (2 bytes)	90	00

Returns the start address and length of loadable EEPROM.

Command-Specific Error Codes in SW1-SW2:

swLcLeError	Lc is present, or Le is absent
swInvalidState	Card is not in NEW or LOAD state
swP1P2Error	P1 <> 00 or P2 <> 00

To call **EEPROM SIZE** from a Terminal program:

```
#Include COMMANDS.DEF
Call EepromSize (Start%, Length%)
```


7. Communications

7.7.4 The CLEAR EEPROM Command

CLEAR EEPROM – Set specified bytes to **FF**

Command syntax:

CLA	INS	P1	P2	Lc	IDATA
C0	04	hi	lo	02	length (2 bytes)

Response:

SW1	SW2
90	00

Sets *length* bytes of EEPROM to **FF**, starting from address *hi:lo*.

Command-Specific Error Codes in SW1-SW2:

swLcLeError	Lc <> 02 , or length of IDATA <> 02
swInvalidState	Card is not in NEW or LOAD state
swOutsideEeprom	Address range not wholly contained in EEPROM

To call **CLEAR EEPROM** from a Terminal program:

```
#Include COMMANDS.DEF
Call ClearEeprom (P1P2=address, Length%)
```


7.7.5 The WRITE EEPROM Command

WRITE EEPROM – Load data into EEPROM

Command syntax:	CLA	INS	P1	P2	Lc	IDATA
	C0	06	<i>hi</i>	<i>lo</i>	<i>len</i>	<i>data</i>

Response:	SW1	SW2
	90	00

Writes *data* (*len* bytes) to EEPROM starting at address *hi:lo*.

Command-Specific Error Codes in SW1-SW2:

swLcLeError **Lc** <> length of **IDATA**
swInvalidState Card is not in **NEW** or **LOAD** state
swOutsideEeprom Address range not wholly contained in EEPROM

To call **WRITE EEPROM** from a Terminal program:

```
Declare Command &HC0 &H06 WriteEeprom(Data$, Disable Le)
Call WriteEeprom (P1P2=address, Data$)
```

Note: For security reasons, the **WRITE_EEPROM** command is encrypted, and is not available for general use. Calling this command from a user program is likely to damage the card irreparably. For this reason, it is not included in COMMANDS.DEF. However, it is possible to call this command with data supplied by the compiler in the Image File – see the **BCLOAD.EXE** source code in BasicCardPro\Source\BCLoad for an example of how to do this. In such cases, you must declare the **WriteEeprom** command yourself, as shown above.

7. Communications

7.7.6 The READ EEPROM Command

READ EEPROM – Read data from EEPROM

Command syntax:

CLA	INS	P1	P2	Le
C0	08	hi	lo	len

Response:

ODATA	SW1	SW2
len bytes	90	00

Reads *len* bytes from EEPROM starting from address *hi:lo*. If you have configured key number **00** in the card, then the **READ EEPROM** command can be called whatever the state of the card, by enabling encryption with key **00**. You should consider this option whenever the card contains data that is not available elsewhere – if the card becomes unusable for any reason, for example because of hardware errors writing to EEPROM, you can recover the data this way.

Command-Specific Error Codes in SW1-SW2:

swLcLeError	Lc is present, or Le is absent
swInvalidState	Card is not in NEW or LOAD state, and key 00 is not active
swOutsideEeprom	Address range not wholly contained in EEPROM

To call **READ EEPROM** from a Terminal program:

```
#Include COMMANDS.DEF
Call ReadEeprom (P1P2=address, Data$, Le=len)
```


7.7.7 The EEPROM CRC Command

EEPROM CRC – Calculate a CRC over a specified EEPROM address range

Command syntax:	CLA	INS	P1	P2	Lc	IDATA	Le
	C0	0A	<i>hi</i>	<i>lo</i>	02	<i>length</i> (2 bytes)	02

Response:	ODATA	SW1	SW2
	<i>CRC</i> (2 bytes)	90	00

Returns the CRC of *length* bytes from address *hi:lo*. All bytes must be in EEPROM. This command can be used to verify the contents of EEPROM after downloading an application to the card.

In the Enhanced BasicCard, this command also serves the function of enabling the BasicCard file system. To access the file system while the card is still in state **LOAD**, an **EEPROM CRC** command must be sent, to let the card know that the relevant data structures have been downloaded; the **BCLOAD** program does this automatically after downloading a ZC-Basic program to the BasicCard.

Warning: Do not call this command in the Enhanced BasicCard before a valid ZC-Basic program has been loaded. The card will attempt to enable a non-existent file system, which can permanently disable the card. (In the Compact and Professional BasicCards, you can call this command at any time.)

Command-Specific Error Codes in SW1-SW2:

swLcLeError	Lc <> 02 or length of IDATA <> 02 or Le not present
swInvalidState	Card is not in NEW or LOAD state
swOutsideEeprom	Address range not wholly contained in EEPROM

To call **EEPROM CRC** from a Terminal program:

```
#Include COMMANDS.DEF
Call EepromCRC (P1P2=address, Length%)
```

The CRC is returned in the **Length%** variable.

Note: If **Le** >= 3, the Professional BasicCard returns a 32-bit CRC. To call the 32-bit **EEPROM CRC** command from a Terminal program:

```
#Include COMMANDS.DEF
CRChi% = length
Call EepromCRC32 (P1P2=address, CRChi%, CRCLo%)
```

16-bit and 32-bit CRC calculations are described in **6.8.4 CRC Calculations**.

7. Communications

7.7.8 The SET STATE Command

SET STATE – Set the state of the card

Command syntax:

CLA	INS	P1	P2
C0	0C	<i>state</i>	00

Response:

SW1	SW2
90	00

This command changes the state of the card, as follows:

Compact and Enhanced BasicCards:

<i>state:</i>	01	02	03
New card state:	LOAD	TEST	RUN

Professional BasicCard:

<i>state:</i>	01	02	03	04
New card state:	LOAD	PERS	TEST	RUN

After this command is successfully called, no further commands are allowed until the card is reset.

Command-Specific Error Codes in SW1-SW2:

swLcLeError	Lc or Le present
swInvalidState	Card is in RUN state
swCardUnconfigured	The card has not been configured by ZeitControl. If you see this error, contact ZeitControl for a replacement card.
swP1P2Error	P1 = 00 or P1 > RUN or P2 <> 00

To call **SET STATE** from a Terminal program:

```
#Include COMMANDS.DEF
Call SetState (P1=State@)
```

Note: This command may also be used to certify EEPROM code in Enhanced BasicCards **ZC3.1**, **ZC3.2**, and **ZC3.31**. Contact ZeitControl if you need to know how this works.

7.7.9 The GET APPLICATION ID Command

GET APPLICATION ID – Get the Application ID string

Command syntax:

CLA	INS	P1	P2	Le
C0	0E	00	00	00

Response:

ODATA	SW1	SW2
<i>Application-ID</i>	61	<i>len</i>

This command returns the Application ID specified in the ZC-Basic source code statement:

Declare ApplicationID = *Application-ID*

Command-Specific Error Codes in SW1-SW2:

swLcLeError	Lc is present or Le is absent
swInvalidState	Card is not in TEST or RUN state
swP1P2Error	P1 <> 00 or P2 <> 00
swDataNotFound	Application ID not configured

To call **GET APPLICATION ID** from a Terminal program:

```
#Include COMMANDS.DEF
Call GetApplicationID (Name$)
```


7. Communications

7.7.10 The START ENCRYPTION Command

START ENCRYPTION – Start automatic encryption of command/response data

Compact and Enhanced BasicCards:

Command syntax:	CLA	INS	P1	P2	Lc	IDATA	Le
	C0	10	<i>algorithm</i>	<i>key</i>	04	Random number RA (4 bytes)	04

Response:	ODATA	SW1	SW2
	Random number RB (4 bytes)	90	00

Professional BasicCard:

Command syntax:	CLA	INS	P1	P2	Lc	IDATA	Le
	C0	10	<i>algorithm</i>	<i>key</i>	<i>len_R</i>	Random number RA (<i>len_R</i> bytes)	00

Response:	ODATA	SW1	SW2
	<i>algorithm</i> (1 byte); Random number RB (<i>len_R</i> bytes)	61	<i>len_R+1</i>

This command initiates automatic encryption of command and response data fields.

algorithm is one of the following cryptographic algorithms:

<i>algorithm</i>		<i>len_R</i>	<i>key length</i>
11	SG-LFSR (Shrinking Generator – Linear Feedback Shift Register)	4	8
12	SG-LFSR with CRC-16	4	8
21	Single DES (Data Encryption Standard, 8-byte key)	4	8
22	Triple DES (Data Encryption Standard, 16-byte key)	4	10 (decimal 16)
31	AES-128 (Advanced Encryption Standard, 128-bit key)	8	10 (decimal 16)
32	AES-192 (Advanced Encryption Standard, 192-bit key)	8	18 (decimal 24)
33	AES-256 (Advanced Encryption Standard, 256-bit key)	8	20 (decimal 32)

For descriptions of these algorithms, and the role of **RA** and **RB**, see **Chapter 8: Encryption Algorithms**.

key is the key number. It must match one of the key numbers configured in the BasicCard program with the ZC-Basic **Declare Key** statement, of length at least *key length* from the above table.

Algorithms supported in the Compact BasicCard

The Compact BasicCard supports algorithms **11** (**SG-LFSR**) and **12** (**SG-LFSR with CRC-16**).

Algorithms supported in the Enhanced BasicCard

The Enhanced BasicCard supports algorithms **21** (**Single DES**) and **22** (**Triple DES**).

Algorithms supported in the Professional BasicCard

The different Professional BasicCard versions support various combinations of cryptographic algorithms. See the **Professional BasicCard Datasheet** for up to date information. At the time of writing, the following versions are available:

<i>BasicCard Version</i>	<i>Algorithms</i>
ZC4.5A	AES-128
ZC4.5D	Single DES, Triple DES
ZC5.4	AES-128, Single DES, Triple DES
ZC5.5	AES-128, AES-192, AES-256, Single DES, Triple DES

Automatic Algorithm Selection

The Professional and Enhanced BasicCards support automatic algorithm selection: If *algorithm* is zero, then the card automatically selects the strongest algorithm that is compatible with *len_R* and the key length. In the Professional BasicCard, the algorithm thus selected is returned in the first byte of **ODATA**.

The Compact BasicCard returns with **SW1-SW2** = **swUnknownAlgorithm** if *algorithm* is zero.

Command-Specific Error Codes in SW1-SW2:

swKeyNotFound	Key number <i>key</i> was not configured
swPolyNotFound	Primitive polynomials were not initialised
swKeyTooShort	Key number <i>key</i> is too short
swKeyDisabled	Key number <i>key</i> is disabled
swUnknownAlgorithm	<i>algorithm</i> is unknown, or is not enabled in the card
swAlreadyEncrypting	Encryption is already enabled
swLcLeError	<i>Compact and Enhanced BasicCards</i> : Lc <> 04 , or Le is absent <i>Professional BasicCard</i> : RA is too short, or Le is absent
swInvalidState	Card is not in TEST or RUN state

To call **START ENCRYPTION** from a Terminal program for a Compact or Enhanced BasicCard, or a Professional BasicCard with **DES** support:

```
#Include COMMANDS.DEF
Call StartEncryption ([P1=Algorithm,] P2=KeyNumber, Rnd)
```

To call **START ENCRYPTION** from a Terminal program for a Professional BasicCard:

```
#Include COMMANDS.DEF
Call ProEncryption ([P1=Algorithm,] P2=KeyNumber, Rnd, Rnd)
```

Note that both forms are accepted by a Professional BasicCard with **DES** support.

Alternatively, **COMMANDS.DEF** defines the subroutine **AutoEncryption**, which automatically selects the correct version of the command:

```
#Include COMMANDS.DEF
Call AutoEncryption (KeyNumber)
```


7. Communications

7.7.11 The END ENCRYPTION Command

END ENCRYPTION – End automatic encryption

Command syntax:

CLA	INS	P1	P2
C0	12	00	00

Response:

SW1	SW2
90	00

This command ends automatic encryption of command and response data fields.

Command-Specific Error Codes in SW1-SW2:

swNotEncrypting	Encryption is not currently enabled
swLcLeError	Lc or Le present
swInvalidState	Card is not in TEST or RUN state
swP1P2Error	P1 <> 00 or P2 <> 00

To call **END ENCRYPTION** from a Terminal program:

```
#Include COMMANDS.DEF
Call EndEncryption()
```


7.7.12 The ECHO Command

ECHO – Echo the command data

Command syntax:	CLA	INS	P1	P2	Lc	IDATA	Le
	C0	14	<i>increment</i>	00	<i>datalen</i>	<i>data</i>	<i>resplen</i>

Response:	ODATA	SW1	SW2
	<i>data+increment</i>	90	00

This command simply adds *increment* to each byte in *data*, and returns *resplen* bytes. It is intended for testing communication and encryption (see **8.9 Encryption – a Worked Example**).

Note: The Compact and Enhanced BasicCards ignore *resplen*, always returning *datalen* bytes.

Command-Specific Error Codes in SW1-SW2:

swLcLeError **Lc** <> length of **IDATA** or **Le** not present
swP1P2Error **P2** <> **00**

To call **ECHO** from a Terminal program:

```
#Include COMMANDS.DEF
Call Echo (P1=increment, S$, Le=resplen)
```


7. Communications

7.7.13 The ASSIGN NAD Command

ASSIGN NAD – Assign a Node Address to the card

Command syntax:

CLA	INS	P1	P2
C0	16	NAD	00

Response:

SW1	SW2
90	00

If $1 \leq NAD \leq 7$, this command tells the card to respond only to those messages in which the high nibble of the first byte (the **NAD**) is equal to *NAD*. If *NAD* = 0, this command tells the card to respond to all messages. Other values of *NAD* are invalid.

Notes:

- The **ASSIGN NAD** command is not used by ZeitControl's software; all commands sent by the Terminal program have **NAD=00**.
- This command is supported only by Compact BasicCard **ZC1.1** and Enhanced BasicCards **ZC3.3** through **ZC3.9**.

Command-Specific Error Codes in SW1-SW2:

swLcLeError	Lc or Le present
swP1P2Error	P1 > 07 or P2 <> 00

To call **ASSIGN NAD** from a Terminal program:

```
#Include COMMANDS.DEF
Call AssignNAD (P1=NAD)
```


7.7.14 The FILE IO Command

FILE IO – Execute a file system operation (Enhanced and Professional BasicCards only)

Command syntax:	CLA	INS	P1	P2	Lc	IDATA	Le
	C0	18	<i>SysCode</i>	<i>filenum</i>	<i>CommandLen</i>	<i>CommandData</i>	<i>ResponseLen</i>

Response:	ODATA	SW1	SW2
	<i>status</i> (1 byte) + <i>ResponseData</i>	90	00

This command is sent whenever the Terminal program attempts to access the file system in the BasicCard. The P-Code interpreter in the PC builds the command automatically, sends it to the BasicCard, and interprets the response. *SysCode* is the same as the *SysCode* parameter to the **SYSTEM** P-Code instruction – see **9.7.4 FILE SYSTEM Functions**. The *status* byte in the **ODATA** field is the **FileError** byte for the operation. The format of the *CommandData* and *ResponseData* fields depends on the value of *SysCode*, and is not described in this document.

Command-Specific Error Codes in SW1-SW2:

swLcLeError **Lc** <> length of **IDATA**, or **Le** absent
swP1P2Error *SysCode* is not a valid file system operation

The **FILE IO** command was not designed to be called directly from a Terminal program. The P-Code interpreter calls it automatically when a file system operation is requested – see **Chapter 4: Files and Directories** for a description of the file system commands available in ZC-Basic.

7.8 The Command Definition File COMMANDS.DEF

The file COMMANDS.DEF can be found in the directory BasicCardPro\Inc. It contains:

- declarations of all the pre-defined commands;
- definitions of the ZC-Basic **SW1-SW2** status codes; and
- definitions of P-Code error codes.

See **7.6 Status Bytes SW1 and SW2** for descriptions of the status and error codes.

Here is the file COMMANDS.DEF:

```
Rem Pre-defined BasicCard commands

#IfNotDef CommandsDefIncluded ' Prevent multiple inclusion
Const CommandsDefIncluded = True

Declare Command &HC0 &H00 GetState(Lc=0, State@, Version$)
Declare Command &HC0 &H02 EepromSize(Lc=0, Start%, Length%)
Declare Command &HC0 &H04 ClearEeprom(Length%, Disable Le)

Rem Since Version 3.01, the WRITE EEPROM command is no longer supported.
Rem Use it at your own risk!
Rem
Rem Declare Command &HC0 &H06 WriteEeprom(Data$, Disable Le)

Declare Command &HC0 &H08 ReadEeprom(Lc=0, Data$)
Declare Command &HC0 &H0A EepromCRC(Length%)
Declare Command &HC0 &H0A EepromCRC32(Lc=2, CRCHi%, CRCLo%, Le=4)
Declare Command &HC0 &H0C SetState()
Declare Command &HC0 &H0E GetApplicationID(Lc=0, Name$)
Declare Command &HC0 &H10 StartEncryption(RA&, Le=0)
Declare Command &HC0 &H12 EndEncryption()
Declare Command &HC0 &H14 Echo(S$)
Declare Command &HC0 &H16 AssignNAD()

Rem BasicCard operating system errors

Const swCommandOK                = &H9000
Const swRetriesRemaining          = &H63C0
Const swEepromWriteError          = &H6581
Const swBadEepromHeap             = &H6582
Const swBadFileChain              = &H6583
Const swKeyNotFound               = &H6611
Const swPolyNotFound              = &H6612
Const swKeyTooShort               = &H6613
Const swKeyDisabled               = &H6614
Const swUnknownAlgorithm          = &H6615
Const swAlreadyEncrypting         = &H66C0
Const swNotEncrypting             = &H66C1
Const swBadCommandCRC            = &H66C2
Const swDesCheckError             = &H66C3
Const swCoprocesorError           = &H66C4
Const swLcLeError                 = &H6700
Const swCommandTooLong            = &H6781
Const swResponseTooLong           = &H6782
Const swInvalidState              = &H6985
Const swCardUnconfigured          = &H6986
Const swNewStateError             = &H6987
Const swPlP2Error                 = &H6A00
Const swOutsideEeprom            = &H6A02
```


7.8 The Command Definition File COMMANDS.DEF

```
Const swDataNotFound          = &H6A88
Const swINSNotFound           = &H6D00
Const swReservedINS           = &H6D80
Const swCLANotFound           = &H6E00
Const swReservedCLA           = &H6E80
Const swInternalError         = &H6F00

Rem SW1=&H61 is Le warning:

Const swlLeWarning            = &H61

Rem SW1=&H6C is La warning (T=0 protocol only):

Const swlLaWarning            = &H6C

Rem P-Code interpreter errors (SW1=&H64, SW2=P-Code error)

Const swlPCodeError           = &H64

Const pcStackOverflow          = &H01
Const pcDivideByZero           = &H02
Const pcNotImplemented         = &H03
Const pcBadRamHeap             = &H04
Const pcBadEepromHeap          = &H05
Const pcReturnWithoutGoSub     = &H06
Const pcBadSubscript           = &H07
Const pcBadBounds              = &H08
Const pcInvalidReal            = &H09
Const pcOverflow               = &H0A
Const pcNegativeSqrt           = &H0B
Const pcDimensionError         = &H0C
Const pcBadStringCall          = &H0D
Const pcOutOfMemory            = &H0E
Const pcArrayNotDynamic        = &H0F
Const pcArrayTooBig            = &H10
Const pcDeletedArray           = &H11
Const pcPCodeDisabled          = &H12
Const pcBadSystemCall          = &H13
Const pcBadKey                 = &H14
Const pcBadLibraryCall         = &H15
Const pcStackUnderflow         = &H16

Rem Error codes generated by the Terminal

Const swNoCardReader           = &H6790
Const swCardReaderError        = &H6791
Const swNoCardInReader         = &H6792
Const swCardPulled             = &H6793
Const swTlError                = &H6794
Const swCardError              = &H6795
Const swCardNotReset           = &H6796
Const swKeyNotLoaded           = &H6797
Const swPolyNotLoaded          = &H6798
Const swBadResponseCRC         = &H6799
Const swCardTimedOut           = &H679A
Const swTermOutOfMemory        = &H679B
Const swBadDesResponse         = &H679C
Const swInvalidComPort         = &H679D
Const swComPortNotSupported    = &H679E
Const swNoPcscDriver           = &H679F
Const swPcscReaderBusy         = &H67A0
```


7. Communications

```
Const swPcscError           = &H67A1
Const swComPortBusy         = &H67A2
Const swBadATR              = &H67A3
Const swT0Error             = &H67A4
Const swPTSError            = &H67A7
Const swDataOverrun         = &H67A8
Const swCommandTooShort     = &H67A9
Const swCommandFormat       = &H67AA
Const swResponseTooShort    = &H67AB
Const swUnexpectedResponse  = &H67AC
Const swInvalidSetState     = &H67AD
Const swTerminalProgramRunning = &H67AE

#EndIf ' CommandsDefIncluded
```


8. Encryption Algorithms

The Compact BasicCard supports the following two encryption algorithms:

Algorithm

11	SG-LFSR (Shrinking Generator – Linear Feedback Shift Register)
12	SG-LFSR with CRC-16

The Enhanced BasicCard supports the following two encryption algorithms:

Algorithm

21	Single DES (Data Encryption Standard, 8-byte key)
22	Triple DES (Data Encryption Standard, 16-byte key)

The Professional BasicCard supports some or all of the following encryption algorithms:

Algorithm

21	Single DES (Data Encryption Standard, 8-byte key)
22	Triple DES (Data Encryption Standard, 16-byte key)
31	AES-128 (Advanced Encryption Standard, 128-bit key)
32	AES-192 (Advanced Encryption Standard, 192-bit key)
33	AES-256 (Advanced Encryption Standard, 256-bit key)

This chapter describes these algorithms in detail, to give interested readers the opportunity to evaluate them. But you don't need to know how these algorithms work in order to use them; if you only want to know how to use them from ZC-Basic, skip this chapter and see instead **3.17.1 Implementing Encryption**.

8.1 The DES Algorithm

The **DES** algorithm is the internationally recognised Data Encryption Standard, defined in the ANSI standard documents *X3.92-1981 (Data Encryption Algorithm)* and *X3.106-1983 (Data Encryption Algorithm – Modes of Operation)*. See these documents for a definition of the **DES** algorithm itself; for a fuller treatment, including 'C' source code, see Bruce Schneier's *Applied Cryptography* (Second Edition, John Wiley & Sons, Inc., 1996).

As you can see from the dates of the ANSI documents, the **DES** algorithm is no longer young. In fact, the original **DES** algorithm is usually referred to as **Single DES**, and must now be regarded as less than completely secure. Special-purpose hardware can be constructed for several tens of thousands of dollars, that can break **Single DES** encryption in less than a day. For this reason, a stronger version, **Triple DES**, has become a *de facto* standard in the banking world. This algorithm is generally believed to be safe against all currently feasible attacks. However, **Single DES** is still used for protecting confidential but financially worthless data, such as a patient's medical records.

The original ANSI X3.92 document defines **DES** as an encryption function that takes a 56-bit key **K** and an 8-byte data block **P** as input, and returns an 8-byte data block **C** as output:

$$C = E_K(P)$$

The inverse of this is the **DES** decryption function:

$$P = D_K(C)$$

(This notation is taken from Bruce Schneier's *Applied Cryptography*: **P** and **C** denote plaintext and ciphertext, **E** and **D** are encryption and decryption, and **K** is the key.)

8. Encryption Algorithms

Note that a **Single DES** key contains only 56 bits, although ZC-Basic requires 8-byte keys. This is usual in **DES** implementations; the top bit of each byte can be used as a parity check, or simply thrown away (which is what the BasicCard does).

The **Triple DES** algorithm takes a 16-byte key and splits it into two 8-byte keys **KL** and **KR**. Then the encryption and decryption functions are given by

$$C = E_K^3(P) = E_{KL}(D_{KR}(E_{KL}(P))) \text{ and}$$

$$P = D_K^3(C) = D_{KL}(E_{KR}(D_{KL}(C)))$$

(The four functions E_K , D_K , E_K^3 , and D_K^3 can be called directly from ZC-Basic – see **3.17.6 DES Encryption Primitives**.)

Given such encryption and decryption functions, there are several ways that they can be used to encrypt and decrypt a message of arbitrary length. The method used by the Enhanced BasicCard is described in the next section.

8.2 Implementation of DES in the BasicCard

Apart from their encryption and decryption functions (E and D versus E^3 and D^3), the implementations of **Single DES** and **Triple DES** in the Enhanced BasicCard are identical. To start with, we need to know how to encrypt a message that is longer than 8 bytes. (All commands and responses encrypted with **DES** in the BasicCard are at least 8 bytes long.)

8.2.1 The Message Encryption Functions ME_K and ME_K^3

The **Single DES** message encryption function $C = ME_K(P)$ is defined as follows. We are given:

- a message P , at least 8 bytes in length;
- an 8-byte key K ;
- the **Single DES** encryption and decryption functions E_K and D_K ;
- an 8-byte *initialisation vector* C_0 (more about this in **8.2.3 The Initialisation Vector**).

First, split the message P into 8-byte blocks P_1, P_2, \dots, P_{n-1} , plus a final block P_n that may be shorter than 8 bytes. Pad this final block with m zeroes to a length of 8 bytes (so $0 \leq m \leq 7$). Then compute, for $1 \leq i \leq n$:

$$C_i = E_K(C_{i-1} \text{ Xor } P_i)$$

(Note that the initialisation vector C_0 is needed to compute C_1 .) Then throw away the last m bytes of the *penultimate* block C_{n-1} , and concatenate the resulting blocks C_1, \dots, C_n to get the encrypted ciphertext C .

If we threw away the last m bytes of the *last* block C_n , then the message C couldn't be decrypted by its recipient. But the recipient can reconstruct the last m bytes of C_{n-1} , as follows:

$$\text{The last block is computed from } C_n = E_K(C_{n-1} \text{ Xor } P_n)$$

$$\text{Therefore, } D_K(C_n) = C_{n-1} \text{ Xor } P_n$$

$$\text{which means that } C_{n-1} = D_K(C_n) \text{ Xor } P_n$$

But the last m bytes of P_n are all zero, so the last m bytes of C_{n-1} are equal to the last m bytes of $D_K(C_n)$, which can be computed without prior knowledge of the plaintext P . This trick is called *ciphertext stealing*, and it allows us to keep encrypted messages to their original size.

The **Triple DES** message encryption function $C = ME_K^3(P)$ is defined in exactly the same way, except that the key K is 16 bytes long, and the **Triple DES** encryption function E^3 is substituted for the **Single DES** function E .

8.2.2 The Message Decryption Functions MD_K and MD_K^3

The **Single DES** message decryption function $P = MD_K(C)$ is the inverse of ME_K . First restore the penultimate block C_{n-1} to 8 bytes, as described in the previous section. Then compute, for $1 \leq i \leq n$:

$$P_i = C_{i-1} \text{ Xor } D_K(C_i)$$

Throw away the last m bytes in P_n (which should all be zero), and concatenate all the resulting blocks P_1, \dots, P_n to get the original plaintext message P .

The **Triple DES** message decryption function $C = MD_K^3(P)$ is defined in exactly the same way, except that the **Triple DES** decryption function D^3 is substituted for the **Single DES** function D .

8.2.3 The Initialisation Vector

The initialisation vector C_0 is determined as follows:

For the first command following a **START ENCRYPTION** command, the initialisation vector C_0 depends on the command and response fields of the **START ENCRYPTION** command:

Command syntax:	CLA	INS	P1	P2	Lc	IDATA	Le
	C0	10	<i>algorithm</i>	<i>key</i>	04	<i>Random number RA</i> (4 bytes)	04

Response:	ODATA	SW1	SW2
	<i>Random number RB</i> (4 bytes)	90	00

In this case, C_0 consists of the first two bytes of **RA**, followed by all four bytes of **RB**, followed by the last two bytes of **RA**.

For subsequent commands and responses, C_0 is simply the last ciphertext block C_n of the previous message.

8.2.4 Encryption of Commands in the Enhanced BasicCard

A command has the following structure (shaded blocks are optional):

CLA	INS	P1	P2	Lc	IDATA	Le
------------	------------	-----------	-----------	-----------	--------------	-----------

Encryption consists of the following steps:

- If the **Lc** or **Le** fields are absent, insert **Lc' = 00** and/or **Le' = 00**:

CLA	INS	P1	P2	Lc'	IDATA	Le'
------------	------------	-----------	-----------	------------	--------------	------------

- Append two zeroes (the resulting command now contains at least 8 bytes):

P =	CLA	INS	P1	P2	Lc'	IDATA	Le'	00	00
------------	------------	------------	-----------	-----------	------------	--------------	------------	-----------	-----------

- Encrypt the whole command **P**, with $C = ME_K(P)$ or $C = ME_K^3(P)$:

C

- Wrap the resulting ciphertext **C** in the original command parameters:

CLA	INS	P1	P2	Lc' + 8	C	Le
------------	------------	-----------	-----------	----------------	----------	-----------

The resulting command is always exactly 8 bytes longer than the original command. These 8 bytes of redundancy enable an authentication check to be done: the command parameters **CLA INS P1 P2 Lc'**

8. Encryption Algorithms

Le' 00 00 in the decrypted command must match the wrapping, otherwise the command is rejected, with **SW1-SW2 = swDesCheckError**.

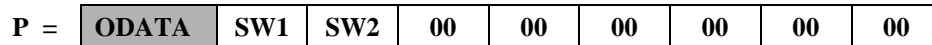
8.2.5 Encryption of Responses in the Enhanced BasicCard

A response has the following structure (the shaded block is optional):



Encryption consists of the following steps:

- Append six zeroes:



- Encrypt the resulting response **P**, with **C = ME_K(P)** or **C = ME_K³(P)**:



- Append the original **SW1-SW2**:



The resulting response is always exactly 8 bytes longer than the original response. As with command encryption, these 8 bytes of redundancy enable an authentication check to be done on the response: if the decrypted response doesn't end with **SW1-SW2** followed by six zeroes, the response is rejected, and **SW1-SW2 = swBadDesResponse** is returned to the caller in the Terminal program.

Note: If status bytes **SW1 SW2** indicate an error (i.e. **SW1SW2 <> swCommandOK** and **SW1 <> sw1LeWarning**), then the response is not encrypted.

8.2.6 Encryption of Commands in the Professional BasicCard

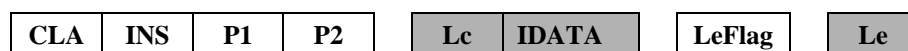
The Professional BasicCard required a new encryption algorithm, because the algorithms described above for the Enhanced BasicCard are not compatible with the **T=0** protocol.

A command has the following structure (shaded blocks are optional):



Encryption consists of the following steps:

- Insert an **LeFlag** byte: **01** if **Le** is present, **00** if **Le** is absent:



- If the **Le** field is absent, append **Le' = 00**:



- Calculate the 32-bit **CRC** of the resulting data:

$$\text{CRC} = \text{CRC32} (\text{CLA} + \text{INS} + \text{P1} + \text{P2} [+ \text{Lc} + \text{IDATA}] + \text{LeFlag} + \text{Le'})$$

The **CRC32** function is defined in **6.8.4 CRC Calculations**.

8.2 Implementation of DES in the BasicCard

- If the **Lc** field is absent, insert **Lc' = 00**:

CLA	INS	P1	P2	Lc'	IDATA	LeFlag	Le'
-----	-----	----	----	-----	-------	--------	-----

- Append two zeroes, followed by the **CRC**:

P =	CLA	INS	P1	P2	Lc'	IDATA	LeFlag	Le'	00	00	CRC
-----	-----	-----	----	----	-----	-------	--------	-----	----	----	-----

- Encrypt the whole command **P**, with $C = ME_K(P)$ or $C = ME_K^3(P)$:

C

- Wrap the resulting ciphertext **C** in the original command parameters:

CLA	INS	P1	P2	Lc' + 8	C	Le''
-----	-----	----	----	---------	---	------

Le'' is computed as follows (this is where **T=0** compatibility comes in):

- If **Le** was absent, then **Le'' = 08**
- If **Le = 00**, then **Le'' = 00**
- Otherwise, **Le'' = Le + 08**

The resulting command is 8 or 9 bytes longer than the original command. When the BasicCard receives the command, it checks that the decrypted data matches the unencrypted command parameters, and that the **CRC** is correct. If not, the command is rejected, with **SW1-SW2 = swDesCheckError**.

8.2.7 Encryption of Responses in the Professional BasicCard

A response has the following structure (the shaded block is optional):

ODATA	SW1	SW2
-------	-----	-----

Encryption consists of the following steps:

- Calculate the 32-bit **CRC** of the response:

$$CRC = CRC32([ODATA] + SW1 + SW2)$$

The **CRC32** function is defined in **6.8.4 CRC Calculations**.

- Append two zeroes and the **CRC**:

P =	ODATA	SW1	SW2	00	00	CRC
-----	-------	-----	-----	----	----	-----

- Encrypt the resulting response **P**, with $C = ME_K(P)$ or $C = ME_K^3(P)$:

C

- Append the original **SW1-SW2**:

C	SW1	SW2
---	-----	-----

The resulting response is always exactly 8 bytes longer than the original response. If the decrypted response doesn't end in **SW1 SW2 00 00 CRC**, the response is rejected, and **SW1-SW2 = swBadDesResponse** is returned to the caller in the Terminal program.

Note: If status bytes **SW1 SW2** indicate an error (i.e. **SW1SW2** \neq **swCommandOK** and **SW1** \neq **sw1LeWarning**), then the response is not encrypted.

8. Encryption Algorithms

8.3 Certificate Generation Using DES

The ZC-Basic **Certificate** command is described in 3.17.7 **Certificate Generation**. The certificate generation algorithm is as follows:

Let **P** be the data to be signed. Append the byte **80** to **P** (this ensures that messages differing only in the number of trailing zeroes will have different certificates). Split the resulting **P** into 8-byte blocks **P**₁ ,..., **P**_n , padding the last block **P**_n with zeroes if necessary. Fill the initialisation vector **C**₀ with zeroes, and then compute, for 1 ≤ i ≤ n:

$$\begin{aligned} C_i &= E_K(C_{i-1} \text{ Xor } P_i) && \text{(for keys } K \text{ shorter than 16 bytes)} \\ C_i &= E_K^3(C_{i-1} \text{ Xor } P_i) && \text{(for keys } K \text{ 16 bytes or longer)} \end{aligned}$$

The certificate is the final ciphertext block **C**_n.

8.4 The AES Algorithm

On 28th February 2001, the US National Institute of Standards and Technology announced the Advanced Encryption Standard (**AES**), the long-awaited replacement for the **DES** standard. **AES** is described in “Draft Federal Information Processing Standard for the AES”. This document is available from NIST’s web site, at <http://csrc.nist.gov/encryption/aes>. **AES** uses the *Rijndael* algorithm as its cryptographic primitive. In its original specification, the Rijndael algorithm encrypts and decrypts data blocks of length 128, 192, or 256 bits, using a key of length 128, 192, or 256 bits. The **AES** specification fixes the block length at 128 bits (i.e. 16 bytes), but retains the three key length options.

AES with a 128-bit key length (or **AES-128**) is considered equal or superior in security to Triple DES. However, it is roughly six times faster. Longer key lengths are correspondingly more secure. For details of how to call the **AES** encryption primitives from a ZC-Basic program, see 6.2 **AES: The Advanced Encryption Standard Library**.

8.5 Implementation of AES in the Professional BasicCard

This section parallels 8.2 **Implementation of DES in the BasicCard**. Here the functions **E**_K and **D**_K are the **AES-xxx** encryption and decryption primitives, where xxx is the key length in bits: 128, 192, or 256. To start with, we need to know how to encrypt a message that is longer than 16 bytes. (All commands and responses encrypted with **AES** in the BasicCard are at least 16 bytes long.)

8.5.1 The Message Encryption Function **AES-ME**_K

The **AES-xxx** message encryption function **C** = **AES-ME**_K(**P**) is defined as follows. We are given:

- a message **P**, at least 16 bytes in length;
- a 16-byte key **K**;
- the **AES-xxx** encryption and decryption functions **E**_K and **D**_K;
- a 16-byte *initialisation vector* **C**₀ (more about this in 8.5.3 **The Initialisation Vector**).

First, split the message **P** into 16-byte blocks **P**₁ , **P**₂ ,..., **P**_{n-1} , plus a final block **P**_n that may be shorter than 16 bytes. Pad this final block with **m** zeroes to a length of 16 bytes (so 0 ≤ **m** ≤ 15). Then compute, for 1 ≤ i ≤ n:

$$C_i = E_K(C_{i-1} \text{ Xor } P_i)$$

(Note that the initialisation vector **C**₀ is needed to compute **C**₁.) Then throw away the last **m** bytes of the *penultimate* block **C**_{n-1} , and concatenate the resulting blocks **C**₁ ,..., **C**_n to get the encrypted ciphertext **C**. For an explanation of why bytes are discarded from the penultimate block, see the description of ciphertext stealing in 8.2.1 **The Message Encryption Functions ME**_K and ME³_K.

8.5.2 The Message Decryption Function $AES-MD_K$

The $AES-xxx$ message decryption function $P = AES-MD_K(C)$ is the inverse of $AES-ME_K$. First restore the penultimate block C_{n-1} to 16 bytes, as described for **DES** in 8.2.1 The Message Encryption Functions ME_K and ME_K^3 . Then compute, for $1 \leq i \leq n$:

$$P_i = C_{i-1} \text{ Xor } D_K(C_i)$$

Throw away the last m bytes in P_n (which should all be zero), and concatenate all the resulting blocks P_1, \dots, P_n to get the original plaintext message P .

8.5.3 The Initialisation Vector

The initialisation vector C_0 is determined as follows:

For the first command following a **START ENCRYPTION** command, the initialisation vector C_0 depends on the command and response fields of the **START ENCRYPTION** command:

Command syntax:	CLA	INS	P1	P2	Lc	IDATA	Le
	C0	10	<i>algorithm</i>	<i>key</i>	08	<i>Random number RA</i> (8 bytes)	00

Response:	ODATA	SW1	SW2
	<i>algorithm</i> (1 byte); <i>Random number RB</i> (8 bytes)	90	00

In this case, C_0 consists of the first four bytes of **RA**, followed by all eight bytes of **RB**, followed by the last four bytes of **RA**.

For subsequent commands and responses, C_0 is simply the last ciphertext block C_n of the previous message.

8.5.4 Encryption of Commands

A command has the following structure (shaded blocks are optional):

CLA	INS	P1	P2	Lc	IDATA	Le
------------	------------	-----------	-----------	-----------	--------------	-----------

Encryption consists of the following steps:

- Insert an **LeFlag** byte: **01** if **Le** is present, **00** if **Le** is absent:

CLA	INS	P1	P2	Lc	IDATA	LeFlag	Le
------------	------------	-----------	-----------	-----------	--------------	---------------	-----------

- If the **Le** field is absent, append **Le' = 00**:

CLA	INS	P1	P2	Lc	IDATA	LeFlag	Le'
------------	------------	-----------	-----------	-----------	--------------	---------------	------------

- Calculate the 32-bit **CRC** of the resulting data:

$$CRC = CRC32 (CLA + INS + P1 + P2 [+ Lc + IDATA] + LeFlag + Le')$$

The **CRC32** function is defined in 6.8.4 CRC Calculations.

- If the **Lc** field is absent, insert **Lc' = 00**:

CLA	INS	P1	P2	Lc'	IDATA	LeFlag	Le'
------------	------------	-----------	-----------	------------	--------------	---------------	------------

8. Encryption Algorithms

- Append ten zeroes, followed by the **CRC**:

$$P =$$

CLA	INS	P1	P2	Lc'	IDATA	LeFlag	Le'	00	...	00	CRC
-----	-----	----	----	-----	-------	--------	-----	----	-----	----	-----

- Encrypt the whole command **P**, with $C = \text{AES-ME}_K(P)$:

C

- Wrap the resulting ciphertext **C** in the original command parameters:

CLA	INS	P1	P2	Lc' + 16	C	Le''
-----	-----	----	----	----------	---	------

Le'' is computed as follows:

- If **Le** was absent, then **Le'' = 10**
- If **Le = 00**, then **Le'' = 00**
- Otherwise, **Le'' = Le + 10**

The resulting command is 16 or 17 bytes longer than the original command. When the BasicCard receives the command, it checks that the decrypted data matches the unencrypted command parameters, and that the **CRC** is correct. If not, the command is rejected, with **SW1-SW2 = swAesCheckError**.

8.5.5 Encryption of Responses

A response has the following structure (the shaded block is optional):

ODATA	SW1	SW2
-------	-----	-----

Encryption consists of the following steps:

- Calculate the 32-bit **CRC** of the response:

$$\text{CRC} = \text{CRC32}([\text{ODATA}] + \text{SW1} + \text{SW2})$$

The **CRC32** function is defined in **6.8.4 CRC Calculations**.

- Append ten zeroes and the **CRC**:

$$P =$$

ODATA	SW1	SW2	00	...	00	CRC
-------	-----	-----	----	-----	----	-----

- Encrypt the resulting response **P**, with $C = \text{AES-ME}_K(P)$:

C

- Append the original **SW1-SW2**:

C	SW1	SW2
---	-----	-----

The resulting response is always exactly 16 bytes longer than the original response. If the decrypted response doesn't end in **SW1 SW2 00...00 CRC**, the response is rejected, and **SW1-SW2 = swBadAesResponse** is returned to the caller in the Terminal program.

Note: If status bytes **SW1 SW2** indicate an error (i.e. **SW1SW2** \neq **swCommandOK** and **SW1** \neq **sw1LeWarning**), then the response is not encrypted.

8.6 The SG-LFSR Algorithm

This algorithm was designed by D. Coppersmith, H. Krawczyk, and Y. Mansour (“The Shrinking Generator”, *Advances in Cryptology – CRYPTO ’93 Proceedings*, Springer-Verlag, 1994). It uses two Linear Feedback Shift Registers, **A** and **S**, to generate a stream of bits: the registers are run in parallel until register **S** generates a **1** bit, at which point the bit generated simultaneously by register **A** is used as the next bit in the stream.

The Compact BasicCard implements this algorithm with Linear Feedback Shift Registers **A** and **S** of length 31 and 32 respectively. In order for the system to be secure against attack with registers of this size, it is necessary to use generating polynomials **PolyA** and **PolyS** that are unknown to the attacker. To this end, we supply a program for the generation of random cryptographic keys and primitive polynomials – see **5.9.4 The Key Generator KEYGEN.EXE**.

C++ source code for the **SG-LFSR** algorithm is provided in the development kit, in the directory `BasicCardPro\Source\SG-LFSR`.

8.7 Implementation of SG-LFSR in the Compact BasicCard

The BasicCard implementation uses primitive polynomials **PolyA** and **PolyS** of degree 31 and 32 respectively, and a cryptographic key **K**, all of which are known only to the two communicating parties. (The **KEYGEN** program generates random polynomials and keys – see **5.9.4 The Key Generator KEYGEN.EXE**.) The **START ENCRYPTION** command is called to enable encryption:

Command syntax:	CLA	INS	P1	P2	Lc	IDATA	Le
	C0	10	<i>algorithm</i>	<i>key</i>	04	<i>Random number RA</i> (4 bytes)	04

Response:	ODATA	SW1	SW2
	<i>Random number RB</i> (4 bytes)	90	00

The caller and responder both contribute 4-byte random numbers to the register initialisation procedure. **RA** may take any value; for maximum security, a different **RA** should be generated for each session. **RB** is generated by the BasicCard.

To describe how the encryption mechanism is initialised, we split all the parts into two-byte words: **RA(0):RA(1)**, **RB(0):RB(1)**, and **K(0):K(1):K(2):K(3)**, where **K** is the (eight-byte) key number *key*.

Then the two registers **A** and **S** are initialised as follows:

```

A(0) = (RA(0) Xor K(0)) And &H7FFF
A(1) = RB(0) Xor K(1)
S(0) = RB(1) Xor K(2)
S(1) = RA(1) Xor K(3)

```

So the initial value of each register depends on both of the random numbers, and on the key.

Zero is an invalid initialisation value, so as a final step:

```

If A(0) = 0 And A(1) = 0 Then A(1) = 1
If S(0) = 0 And S(1) = 0 Then S(1) = 1

```

Encryption starts with the first command after the **START ENCRYPTION** command is received, and remains in effect for commands and responses until an **END ENCRYPTION** command is received (the responses to the **START ENCRYPTION** and **END ENCRYPTION** commands themselves are not encrypted). A ZC-Basic command can tell what kind of encryption is currently active, by looking at the pre-defined variables **Encryption** (the algorithm ID) and **KeyNumber**. (If encryption is currently inactive, then **Encryption** is zero.) Encryption and decryption are identical, and consist of **Xor**-ing each byte with the result of the function `SG_LFSR::GetByte()` (defined in the C++ source file `BasicCardPro\Source\SG-LFSR\sg_lfsr.cpp`).

8. Encryption Algorithms

A command has the following structure (shaded blocks are optional):



Only the data field **IDATA** is encrypted. The command bytes **CLA**, **INS**, **P1**, **P2**, **Lc**, and **Le** are not encrypted, for two reasons:

- The value of these bytes is often predictable. The number of predictable bytes that are encrypted should be kept as low as possible, to make it harder to break the key.
- Compatibility with ISO standards is lost if these bytes are altered.

A response has the following structure (the shaded block is optional):



Again, only the data field **ODATA** is encrypted. The status bytes **SW1** and **SW2** are not encrypted.

8.8 SG-LFSR with CRC

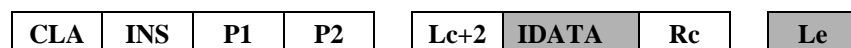
The **SG-LFSR** algorithm is simple to implement, and runs efficiently. However, it provides no authentication for the data it encrypts – I don't need to know the key in order to send encrypted messages. It's true that I won't know what I'm sending, and I won't understand the response. But I could still cause problems by sending random data. If authentication is important (and it usually is), then you should use encryption algorithm 12: **SG-LFSR with CRC** (Cyclic Redundancy Check). The same 16-bit CRC is used as in the **EEPROM CRC** command. 'C' source code for calculating the CRC is given in **6.8.4 CRC Calculations**.

A command has the following structure (shaded blocks are optional):

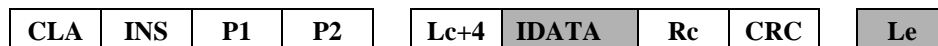


It is encrypted as follows:

- A two-byte random number **Rc** is appended to **IDATA**, and **Lc** is amended accordingly. (Without this random number, the CRC would be predictable in the case of a command with no **IDATA** field. As the CRC is later encrypted, we want to avoid this.)



- The CRC is calculated over the whole of the resulting message (**CLA INS P1 P2 Lc+2 IDATA Rc Le**). It is then appended to the two-byte random number, and **Lc** is updated accordingly.



- The resulting message is encrypted using **SG-LFSR**, as described in section 8.7.

A response has the following structure (the shaded block is optional):



It is encrypted in a similar fashion:

- A two-byte random number **Rr** is appended to **ODATA**.



- The CRC is calculated over the whole of the resulting response (**ODATA Rr SW1 SW2**), and appended to the two-byte random number.



- The resulting response is encrypted using **SG-LFSR**, as described in section 8.7.

Note: If status bytes **SW1 SW2** indicate an error (i.e. **SW1SW2** \neq **swCommandOK** and **SW1** \neq **sw1LeWarning**), then the response is not encrypted.

8.9 Encryption – a Worked Example

This section shows the progression from ZC-Basic source code to encrypted messages. All source files are supplied with the software development kit, in the `BasicCardPro\Examples\echotest` directory.

8.9.1 The Source Code

We ran the **KEYGEN** program to generate encryption polynomials and two cryptographic keys:

```
KEYGEN TESTKEYS -K99 -K100(16) -P
```

This produced output file `TESTKEYS.BAS`:

```
Declare Polynomials = &H609FBB9C,&HD23B770D
Declare Key 99 = &H3E,&H1F,&HA7,&H55,&H81,&HDB,&HC3,&H25
Declare Key 100(16) = &H83,&H24,&H24,&H59,&H86,&H8B,&H8F,&H3F,_
                    &HA0,&HC4,&H1B,&HFE,&H3E,&HF4,&HE2,&H16
```

We edited this file so that it could be included in a Compact BasicCard program:

```
Declare Polynomials = &H609FBB9C,&HD23B770D
Declare Key 99 = &H3E,&H1F,&HA7,&H55,&H81,&HDB,&HC3,&H25

#IfNotDef CompactBasicCard ' 16-bit keys not allowed in Compact BasicCard
Declare Key 100(16) = &H83,&H24,&H24,&H59,&H86,&H8B,&H8F,&H3F,_
                    &HA0,&HC4,&H1B,&HFE,&H3E,&HF4,&HE2,&H16
#EndIf
```

Then we wrote a simple ZC-Basic Terminal program `ECHOTEST.BAS` to send encrypted **ECHO** commands. The `ECHOTEST` program takes a single command-line parameter:

```
ECHOTEST 0 No encryption
ECHOTEST 1 Tests SG-LFSR encryption in the Compact BasicCard
ECHOTEST 2 Tests DES encryption in the Enhanced BasicCard
ECHOTEST 3 Tests DES encryption with CRC in the Professional BasicCard
ECHOTEST 4 Tests AES-128 encryption in the Professional BasicCard
```

We examine the first three cases (**0**, **1**, and **2**) in detail below.

The BasicCard program `ECHOCARD.BAS` just includes the key file:

```
#Include TESTKEYS.BAS
```


8. Encryption Algorithms

8.9.2 The Log Files

The COMPILE.BAT batch file in the source directory creates a Terminal program image file ECHOTEST.IMG, and two BasicCard program image files COMPACT.IMG and ENHANCED.IMG:

```
..\..\ZCMBasic EchoTest -OI -I..\..\Inc
..\..\ZCMBasic EchoCard -OICompact.IMG -CC1 -I..\..\Inc
..\..\ZCMBasic EchoCard -OEnhanced.IMG -CE1 -I..\..\Inc
```

The SIM.BAT batch file runs the EHCOTEST program three times, and creates the I/O log files PLAIN.LOG, COMPACT.LOG, and ENHANCED.LOG:

```
..\..\ZCMSim -CCompact -LPlain EchoTest 0
..\..\ZCMSim -CCompact -LCompact EchoTest 1
..\..\ZCMSim -CEnhanced -LEnhanced EchoTest 2
```

These were the resulting log files. (*Note:* If you run the ECHOTEST program yourself, your log files will be different, due to the different random numbers generated.)

PLAIN.LOG:

```
1: <- 3B EF 00 FF 81 31 20 45 42 61 73 69 63 43 61 72 64 20 5A 43 31 2E 31 BE
2: -> 00 00 09 C0 14 01 00 03 61 62 63 00 BF
   <- 00 00 05 62 63 64 61 03 02
```

COMPACT.LOG:

```
3: <- 3B EF 00 FF 81 31 20 45 42 61 73 69 63 43 61 72 64 20 5A 43 31 2E 31 BE
4: -> 00 40 0A C0 10 11 63 04 29 23 BE 84 04 D8
   <- 00 40 06 E1 6C D6 AE 90 00 23
5: -> 00 00 09 C0 14 01 00 03 E5 D6 30 00 DC
   <- 00 00 05 A2 A5 92 61 03 F2
6: -> 00 40 04 C0 12 00 00 96
   <- 00 40 02 90 00 D2
7: -> 00 00 0A C0 10 12 63 04 52 90 49 F1 04 D1
   <- 00 00 06 F1 BB E9 EB 90 00 DE
8: -> 00 40 0D C0 14 01 00 07 92 98 33 C7 32 39 35 00 5F
   <- 00 40 09 1F C1 1C 13 8F F0 E7 61 03 62
9: -> 00 00 09 C0 12 00 00 04 BC E2 DD C5 99
   <- 00 00 02 90 00 92
```

ENHANCED.LOG:

```
10: <- 3B EF 00 FF 81 31 20 45 42 61 73 69 63 43 61 72 64 20 5A 43 32 2E 31 BF
11: -> 00 40 0A C0 10 21 63 04 A3 F7 76 62 04 98
   <- 00 40 06 C7 F1 B5 02 90 00 57
12: -> 00 00 11 C0 14 01 00 0B D1 2D DB 39 92 7D E3 43 EA 75 C8 00 C9
   <- 00 00 0D BE BD C6 51 0C F8 C7 F3 AF A0 CF 61 03 FB
13: -> 00 40 0D C0 12 00 00 08 34 70 7C 93 08 82 9B 89 A4
   <- 00 40 02 90 00 D2
14: -> 00 00 0A C0 10 22 64 04 FF 7D EA 1A 04 EE
   <- 00 00 06 91 82 D0 F9 90 00 AC
15: -> 00 40 11 C0 14 01 00 0B C6 40 78 CA E4 BC A2 DE 79 05 29 00 CA
   <- 00 40 0D D5 EC EB E4 B8 84 90 6F 6D 0D 8D 61 03 37
16: -> 00 00 0D C0 12 00 00 08 F6 F8 43 29 1E A9 47 38 7B
   <- 00 00 02 90 00 92
```

- 1: **ATR** (Answer To Reset) from the simulated BasicCard, including the text “**BasicCard ZC1.1**”
- 2: Unencrypted **ECHO** command and response
- 3: **START ENCRYPTION** command (algorithm = **&H11**) and response
- 4: Encrypted **ECHO** command and response (algorithm = **&H11**)
- 5: **END ENCRYPTION** command and response
- 6: **ATR** from the simulated Compact BasicCard, as in **1** above.
- 7: **START ENCRYPTION** command (algorithm = **&H12**) and response

- 8: Encrypted **ECHO** command and response (algorithm = **&H12**)
- 9: **END ENCRYPTION** command and response
- 10: **ATR** from the simulated Enhanced BasicCard, including the text “**BasicCard ZC2.1**”
- 11: **START ENCRYPTION** command (algorithm = **&H21**) and response
- 12: Encrypted **ECHO** command and response (algorithm = **&H21**)
- 13: **END ENCRYPTION** command and response
- 14: **START ENCRYPTION** command (algorithm = **&H22**) and response
- 15: Encrypted **ECHO** command and response (algorithm = **&H22**)
- 16: **END ENCRYPTION** command and response

We will look at these commands one by one, disregarding the **T=1** parameters **NAD PCB LEN . . . LRC** in every message.

8.9.3 Unencrypted ECHO Command and Response

The parameter “abc” is **61 62 63** in hexadecimal. The **ECHO** command adds **P1=01** to every byte:

Command:	CLA	INS	P1	P2	Lc	IDATA	Le
	C0	14	01	00	03	61 62 63	00

Response:	ODATA	SW1	SW2
	62 63 64	61	03

8.9.4 START ENCRYPTION (Algorithm = &H11)

The **Rnd** function in the Terminal program returned **RA = &H2923BE84**, and the random-number generator in the BasicCard operating system returned **RB = &HE16CD6AE**. This led to the following **START ENCRYPTION** command-response pair:

Command:	CLA	INS	P1	P2	Lc	IDATA	Le
	C0	10	11	63	04	29 23 BE 84	04

Response:	ODATA	SW1	SW2
	E1 6C D6 AE	90	00

Together with the polynomials and key 99 from file KEYS.BAS:

```
Declare Polynomials = &H609FBB9C,&HD23B770D
Declare Key 99 = &H3E,&H1F,&HA7,&H55,&H81,&HDB,&HC3,&H25
```

we now have all the data we need to initialise the SG_LFSR encryptor. As described in section 8.7, we build the **A** and **S** registers from the following two-byte words:

```
RA(0) = 2923, RA(1) = BE84
RB(0) = E16C, RB(1) = D6AE
K(0) = 3E1F, K(1) = A755, K(2) = 81DB, K(3) = C325
```

Then

```
A(0) = (RA(0) Xor K(0)) And &H7FFF = 173C
A(1) = RB(0) Xor K(1) = 4639
S(0) = RB(1) Xor K(2) = 5775
S(1) = RA(1) Xor K(3) = 7DA1
```

Now the Terminal program operating system initialises its **SG-LFSR** encryptor, first with the polynomials **PolyA** and **PolyS**, and then with the registers **A** and **S**:

```
SG_LFSR Encryptor (0x609FBB9CL, 0xD23B770DL) ;
Encryptor.Initialise (0x173C4639L, 0x57757DA1L) ;
```

(C++ source code for the SG_LFSR class is provided in the development kit – see 8.6 The SG-LFSR Algorithm.) The **IDATA** and **ODATA** sections of subsequent commands and responses will be

8. Encryption Algorithms

encrypted by **Xor**-ing them with successive bytes returned by `Encryptor.GetByte()`. The initialisation values given here generate the sequence:

84 B4 53 C0 C6 F6...

8.9.5 Encrypted ECHO Command (Algorithm = &H11)

From the above sequence, the **IDATA** and **ODATA** sections of the encrypted **ECHO** command and response will be:

61 Xor 84 = E5, 62 Xor B4 = D6, 63 Xor 53 = 30
62 Xor C0 = A2, 63 Xor C6 = A5, 64 Xor F6 = 92

So the **ECHO** command and response will be:

Command:	CLA	INS	P1	P2	Lc	IDATA	Le
	C0	14	01	00	03	E5 D6 30	00

Response:	ODATA	SW1	SW2
	A2 A5 92	61	03

8.9.6 END ENCRYPTION

Before calling **START ENCRYPTION** for algorithm **&H12**, the **END ENCRYPTION** command must be called to cancel the currently enabled encryption. It has no **IDATA** or **ODATA** field, so it is not affected by encryption algorithm **&H11**:

Command:	CLA	INS	P1	P2
	C0	12	00	00

Response:	SW1	SW2
	90	00

8.9.7 START ENCRYPTION (Algorithm = &H12)

This time, the **Rnd** function in the Terminal program returned **RA = &H529049F1**, and the random-number generator in the BasicCard operating system returned **RB = &HF1BBE9EB**. This led to the following **START ENCRYPTION** command-response pair:

Command:	CLA	INS	P1	P2	Lc	IDATA	Le
	C0	10	12	63	04	52 90 49 F1	04

Response:	ODATA	SW1	SW2
	F1 BB E9 EB	90	00

We repeat the process from section **8.9.4** to generate the new **A** and **S** registers:

RA(0) = 5290, RA(1) = 49F1
RB(0) = F1BB, RB(1) = E9EB
K(0) = 3E1F, K(1) = A755, K(2) = 81DB, K(3) = C325

A(0) = (RA(0) Xor K(0)) And &H7FFF = 6C8F
A(1) = RB(0) Xor K(1) = 56EE
S(0) = RB(1) Xor K(2) = 6830
S(1) = RA(1) Xor K(3) = 8AD4

8.9 Encryption – a Worked Example

So the Terminal program operating system re-initialises its **SG-LFSR** encryptor:

```
Encryptor.Initialise (0x6C8F56EEL, 0x68308AD4L) ;
```

and the sequence generated this time is

F3 FA 50 74 94 0F 45 7D A2 78 C8 B3 82 61 3B EE 99 40...

8.9.8 Encrypted ECHO Command (Algorithm = &H12)

The unencrypted **ECHO** command:

Command:	CLA	INS	P1	P2	Lc	IDATA	Le
	C0	14	01	00	03	61 62 63	00

- Add a two-byte random number **Rc**, and set **Lc = 05**:

CLA	INS	P1	P2	Lc	IDATA	Rc	Le
C0	14	01	00	05	61 62 63	B3 A6	00

- Add the CRC calculated over **C0 14 01 00 05 61 62 63 B3 A6 00**, and set **Lc = 07**:

CLA	INS	P1	P2	Lc	IDATA	Rc	CRC	Le
C0	14	01	00	07	61 62 63	B3 A6	36 70	00

- Encrypt **IDATA Rc CRC** with the **SG-LFSR** sequence **F3 FA 50 74 94 0F 45** to get the final version:

CLA	INS	P1	P2	Lc	IDATA	Rc	CRC	Le
C0	14	01	00	07	92 98 33	C7 32	39 35	00

The unencrypted response to the **ECHO** command:

Response:	ODATA	SW1	SW2
	62 63 64	61	03

- Add a two-byte random number **Rr**:

ODATA	Rr	SW1	SW2
62 63 64	DB 3C	61	03

- Add the CRC calculated over **62 63 64 DB 3C 61 03**:

ODATA	Rr	CRC	SW1	SW2
62 63 64	DB 3C	72 86	61	03

- Encrypt **ODATA Rr CRC** with the **SG-LFSR** sequence **7D A2 78 C8 B3 82 61**:

ODATA	Rr	CRC	SW1	SW2
1F C1 1C	13 8F	F0 E7	61	03

8. Encryption Algorithms

8.9.9 END ENCRYPTION

This time, the **END ENCRYPTION** command is affected by the encryption algorithm. The unencrypted **END ENCRYPTION** command:

Command:

CLA	INS	P1	P2
C0	12	00	00

- Add a two-byte random number **Rc**, and set **Lc = 02**:

CLA	INS	P1	P2	Lc	Rc
C0	12	00	00	02	87 0C

- Add the CRC calculated over **C0 12 00 00 02 87 0C**, and set **Lc = 04**:

CLA	INS	P1	P2	Lc	Rc	CRC
C0	12	00	00	04	87 0C	44 85

- Encrypt **Rc CRC** with the **SG-LFSR** sequence **3B EE 99 40**:

CLA	INS	P1	P2	Lc	Rc	CRC
C0	12	00	00	04	BC E2	DD C5

The response is not encrypted:

Response:

SW1	SW2
90	00

8.9.10 START ENCRYPTION (Algorithm = &H21)

This time, the **Rnd** function in the Terminal program returned **RA = &HA3F77662**, and the random-number generator in the BasicCard operating system returned **RB = &HC7F1B502**:

Command:

CLA	INS	P1	P2	Lc	IDATA	Le
C0	10	12	63	04	A3 F7 76 62	04

Response:

ODATA	SW1	SW2
C7 F1 B5 02	90	00

So the initialisation vector **C₀** is loaded with **A3 F7 C7 F1 B5 02 76 62**.

8.9.11 Encrypted ECHO Command (Algorithm = &H21)

The unencrypted **ECHO** command:

Command:

CLA	INS	P1	P2	Lc	IDATA	Le
C0	14	01	00	03	61 62 63	00

8.9 Encryption – a Worked Example

- Add two zeroes:

CLA	INS	P1	P2	Lc	IDATA	Le	
C0	14	01	00	03	61 62 63	00	00 00

- Now we must encrypt the plaintext message $P = C0\ 14\ 01\ 00\ 05\ 61\ 62\ 63\ 00\ 00\ 00$ using the **Single DES** message encryption function ME_K . Referring back to 8.2.1 The Message Encryption Functions ME_K and ME_K^3 :

$K = 3E\ 1F\ A7\ 55\ 81\ DB\ C3\ 25$

$C_0 = A3\ F7\ C7\ F1\ B5\ 02\ 76\ 62$

$P_1 = C0\ 14\ 01\ 00\ 03\ 61\ 62\ 63$

$P_2 = 00\ 00\ 00\ (00\ 00\ 00\ 00\ 00)$

$m = 5$

is key number 99 from TESTKEYS.BAS;

from the **START ENCRYPTION** command;

is the first message block;

is the second message block;

is the length of padding required in P_2 .

So we compute (you can check these in ZC-Basic, using the **DES** function):

$C_1 = E_K(C_0 \text{ Xor } P_1) = E_K(63\ E3\ C6\ F1\ B6\ 63\ 14\ 01) = D1\ 2D\ DB\ 19\ 3E\ 80\ B1\ FB$

$C_2 = E_K(C_1 \text{ Xor } P_2) = E_K(D1\ 2D\ DB\ 19\ 3E\ 80\ B1\ FB) = 39\ 92\ 7D\ E3\ 43\ EA\ 75\ C8$

and we throw away the last m bytes of C_1 to get:

$C = ME_K(P) = D1\ 2D\ DB\ 39\ 92\ 7D\ E3\ 43\ EA\ 75\ C8$

- To get the final version, C is wrapped in the original **CLA INS P1 P2 . . . Le**, with Lc adjusted appropriately:

CLA	INS	P1	P2	Lc	C	Le
C0	14	01	00	0B	D1 2D DB 39 92 7D E3 43 EA 75 C8	00

The unencrypted response to the **ECHO** command:

Response:	ODATA	SW1	SW2
	62 63 64	61	03

- Add six zeroes:

ODATA	SW1	SW2	
62 63 64	61	03	00 00 00 00 00 00

- Encrypt $P = 62\ 63\ 64\ 61\ 03\ 00\ 00\ 00\ 00\ 00\ 00$ using ME_K , where

$K = 3E\ 1F\ A7\ 55\ 81\ DB\ C3\ 25$

$C_0 = 39\ 92\ 7D\ E3\ 43\ EA\ 75\ C8$

$P_1 = 62\ 63\ 64\ 61\ 03\ 00\ 00\ 00$

$P_2 = 00\ 00\ 00\ (00\ 00\ 00\ 00\ 00)$

$m = 5$

is key number 99 from TESTKEYS.BAS;

is C_2 from the **ECHO** command just received;

is the first message block;

is the second message block;

is the length of padding required in P_2 .

So we compute:

$C_1 = E_K(C_0 \text{ Xor } P_1) = E_K(5B\ F1\ 19\ 82\ 40\ EA\ 75\ C8) = BE\ BD\ C6\ 6C\ 9E\ B0\ 59\ F2$

$C_2 = E_K(C_1 \text{ Xor } P_2) = E_K(BE\ BD\ C6\ 6C\ 9E\ B0\ 59\ F2) = 51\ 0C\ F8\ C7\ F3\ AF\ A0\ CF$

and we throw away the last m bytes of C_1 to get:

$C = ME_K(P) = BE\ BD\ C6\ 51\ 0C\ F8\ C7\ F3\ AF\ A0\ CF$

8. Encryption Algorithms

- Now the original **SW1-SW2** are appended, to get:

C	SW1	SW2
BE BD C6 51 0C F8 C7 F3 AF A0 CF	61	03

8.9.12 END ENCRYPTION

The unencrypted **END ENCRYPTION** command:

Command:	CLA	INS	P1	P2
	C0	12	00	00

- Add **Lc' = 00**, **Le' = 00**, and two zeroes:

CLA	INS	P1	P2	Lc'	Le'	
C0	12	00	00	00	00	00 00

- Encrypt **P = C0 12 00 00 00 00 00 00** with **ME_K**, where

K = 3E 1F A7 55 81 DB C3 25
C₀ = 51 0C F8 C7 F3 AF A0 CF
P₁ = C0 12 00 00 00 00 00 00
m = 0

is key number 99 from TESTKEYS.BAS;
 is **C₂** from the **ECHO** response;
 is the only message block;
 is the length of padding required in **P₁**.

So we compute:

$$C_1 = E_K(C_0 \text{ Xor } P_1) = E_K(91 \ 1E \ F8 \ C7 \ F3 \ AF \ A0 \ CF) = 34 \ 70 \ 7C \ 93 \ 08 \ 82 \ 9B \ 89$$

and **C = ME_K(P)** is simply **C₁**.

- The final version:

CLA	INS	P1	P2	Lc	C
C0	12	00	00	08	34 70 7C 93 08 82 9B 89

(**Le** is not appended in this case, because it wasn't present in the unencrypted command.)

The response is not encrypted:

Response:	SW1	SW2
	90	00

8.9.13 Triple DES (Algorithm = &H22)

The three commands (**START ENCRYPTION**, **ECHO**, and **END ENCRYPTION**) are encrypted in exactly the same way for **Triple DES** as for **Single DES**, with two exceptions:

- Triple DES** requires a 16-byte key, so key number 100 is used instead of key number 99;
- the **Triple DES** message encryption function **ME_K³** is substituted for **ME_K**.

9. The ZC-Basic Virtual Machine

Note: Throughout this chapter, **bold** numbers are hexadecimal.

9.1 The BasicCard Virtual Machine

9.1.1 The Compact BasicCard

The Compact BasicCard contains **100** bytes of RAM (= 256 in decimal), and **3E0** bytes of EEPROM (= 992 in decimal). Of this, the operating system uses the first **47** bytes of RAM and the first **23** bytes of EEPROM. The memory available for use by an application written in ZC-Basic is thus **B9** bytes of RAM and **3BD** bytes of EEPROM.

9.1.2 The Enhanced BasicCard

The Enhanced BasicCard contains **100** bytes of RAM (= 256 in decimal), and up to **3FE0** bytes of EEPROM (= 16352 in decimal). Of this, the operating system uses the first **6B** bytes of RAM, and the first **15D** bytes of EEPROM. If the file system is not disabled, it requires **7** bytes of RAM, plus **6** bytes for each file slot. (Files and directories themselves are allocated from the **EEPHEAP** region.)

9.1.3 The Professional BasicCard

The Professional BasicCard contains up to **800** bytes of RAM (= 2048 in decimal), and up to **7FE0** bytes of EEPROM (= 32736 in decimal). The amount of RAM and EEPROM used by the operating system varies from version to version, but the figures in **9.1.2 The Enhanced BasicCard** give a rough guide.

9.1.4 Memory Layout in the BasicCard

RAM and EEPROM are divided into regions, in the following order:

RAM Regions		EEPROM Regions	
RAMSYS	System RAM	EEPSYS	System EEPROM
STACK	The P-Code stack	STRVAL	Single-to-String code*
RAMDATA	Public and Static data	CMDTAB	Command descriptor table
RAMHEAP	Run-time memory allocation	PCODE	The ZC-Basic program code
FILEINFO	Open file slots and file system work-space (Enhanced BasicCard only)	STRCON	String constants
(FRAME)	Procedure frame (contained in STACK)	KEYTAB	Keys for encryption
		EEPDATA	Eeprom data
		EEPHEAP	Run-time memory allocation
		Libraries	Plug-In Libraries

* The **STRVAL** region is only present for Enhanced BasicCard programs that use Single-to-String conversion – see **3.23.5 Single-to-String Conversion**.

The ZC-Basic compiler calculates how much static memory is required for each region, and assigns any remaining memory to **RAMHEAP** and **EEPHEAP**, for run-time memory allocation of strings, arrays, and files. The map file lists the sizes of all these regions – see **10.4 Map File Format**.

9.2 The Terminal Virtual Machine

A Terminal program contains a **CODE** segment and a **DATA** segment, each of which may be up to 64 kilobytes long. The **CODE** segment contains only the **PCODE** region. The **DATA** segment contains

9. The ZC-Basic Virtual Machine

RAM and EEPROM regions (see **2.2.4 Permanent Data** for the meaning of EEPROM data in a Terminal program). The regions occur in the following order (RAM before EEPROM):

RAM Regions		EEPROM Regions	
STACK	The P-Code stack	EEPDATA	Eeprom data
RAMSYS	System RAM	EEPHEAP	Run-time memory allocation
RAMDATA	Public and Static data		
RAMHEAP	Run-time memory allocation		
STRCON	String constants		
(FRAME)	Procedure frame (contained in STACK)		

9.3 The P-Code Stack

The P-Code Virtual Machine has three registers:

PC	Program counter (2 bytes)
SP	Stack Pointer (1 or 2 byte)
FP	Frame Pointer (1 or 2 bytes)

SP and **FP** are 1 byte if RAM is 256 bytes (the Compact and Enhanced BasicCards), otherwise 2 bytes (the Professional BasicCard and the Terminal).

The P-Code stack grows upwards; the **SP** register contains the address of the first free byte on the stack. The stack contains four kinds of data:

- Command parameters, received from the I/O port (BasicCard only). These are located at the bottom of the stack.
- Procedure parameters and return addresses. Before a procedure is called, its parameters are pushed onto the P-Code stack. (If the procedure is a **Function**, space is reserved below the parameters for the function return value.)
- **FRAME** data, consisting of **Private** data and compiler-generated temporary variables. Each procedure has its own **FRAME** region, of a fixed size, that is allocated from the stack when the procedure is called. The **FP** register points to the base of the **FRAME** region.
- Intermediate results of computations. The Virtual Machine has no data registers; all computation is performed on the top of the P-Code stack.

The first P-Code instruction in a procedure is

ENTER *frame-size*

This instruction sets up the **FRAME** region as follows:

- Push **FP**
- Push $\mathbf{SP} + \text{frame-size} + \text{size of SP}$ (i.e. $\mathbf{SP} + \text{frame-size} + 1$ or $\mathbf{SP} + \text{frame-size} + 2$)
- $\mathbf{FP} = \mathbf{SP}$
- $\mathbf{SP} = \mathbf{SP} + \text{frame-size}$

The last instruction in every procedure is

LEAVE

This undoes the effect of the **ENTER** instruction before returning to the caller:

- $\mathbf{SP} = \mathbf{FP} - \text{size of FP}$ (i.e. $\mathbf{FP} - 1$ or $\mathbf{FP} - 2$)
- Pop **FP**
- Pop **PC**

9.4 Run-Time Memory Allocation

The Virtual Machine has two heaps for the run-time allocation of strings and arrays: **RAMHEAP** and **EEPHEAP**. Each is composed of variable-length blocks, that are either *allocated* or *free*; adjacent free blocks are concatenated as soon as they are created. In addition, an allocated block in **EEPHEAP** is either *permanent* or *temporary*. Each block consists of a *block header* followed by a *data area*. The block header contains the length of the data area, and one or two bits describing the block:

EEPHEAP block			RAMHEAP block (small RAM)		RAMHEAP block (large RAM)	
F	T	Len (14 bits)	F	Len (7 bits)	F	Len (15 bits)
Data area (Len bytes)			Data area (Len bytes)		Data area (Len bytes)	

F = **1** if the block is free, **0** if the block is allocated.

T = **1** if the block is temporary, **0** if the block is permanent. A temporary block is automatically freed the next time the BasicCard is reset or the Terminal program is run.

Note: If **F** is **1**, then **T** is not used as a temporary block flag. This means that, although allocated blocks in **EEPHEAP** are limited to 16383 bytes, a free block (and thus the total size of the heap) may be up to 32767 bytes long.

9.5 Data Types

The BasicCard Virtual Machine implements the following data types:

CHAR	1-byte unsigned integer
WORD	2-byte signed integer
LONG	4-byte signed integer
REAL	4-byte IEEE-format floating-point number
STRING	See <i>Strings</i> below

These types correspond to the ZC-Basic data types **Byte**, **Integer**, **Long**, **Single**, and **String** respectively. Arithmetic operations are provided for **WORD**, **LONG**, and **REAL** data; **CHAR** data must be converted to **WORD** before performing arithmetic on it.

9.5.1 Strings

There are two types of string: variable-length and fixed-length.

- A variable-length string is a 2-byte pointer to a Pascal-type string, which consists of a length byte followed by the string contents.
- A fixed-length string is a sequence of characters, whose length is known at compile time.

Both types are restricted to 254 bytes in length; if an operation would result in a longer string, it truncates the result.

String variables take various forms, depending on the storage type:

Eeprom A fixed-length **Eeprom** string variable is a sequence of characters in the **EEPDATA** region. A variable-length **Eeprom** string variable is a 2-byte pointer, in the **EEPDATA** region, to a Pascal-type string in the **EEPHEAP** region.

Public, Static A fixed-length **Public** or **Static** string variable is a sequence of characters in the **RAMDATA** region. A variable-length **Public** or **Static** string variable is a 2-byte pointer, in the **RAMDATA** region, to a Pascal-type string, which

9. The ZC-Basic Virtual Machine

may be in **RAMHEAP** or **EEPHEAP**. Strings are allocated from **RAMHEAP** if there is room, but if not they are allocated from **EEPHEAP**. In this case they are marked as temporary, so that they can be deleted when the BasicCard is reset or the Terminal program is restarted.

Private

A fixed-length **Private** string variable is a sequence of characters in the **FRAME** region. A variable-length **Private** string variable is a 2-byte pointer, in the **FRAME** region, to a Pascal-type string, which may be in **RAMHEAP** or **EEPHEAP**.

String parameters

A **String** parameter takes up 3 bytes on the stack: a one-byte *length* followed by a two-byte *address*. If *length* \leq 254, the address points directly to a fixed-length string. If *length* = 255, the address is a handle, and points to a variable-length string variable. (This is the reason for the 254-byte length restriction on all strings.)

9.6 P-Code Instructions

In this section, names in *italics* obey the following conventions:

- Initial characters *s* and *u* denote signed and unsigned values respectively.
- Initial character *r*, or second character *c*, *w*, *l*, denote **REAL**, **CHAR**, **WORD**, and **LONG** data respectively.
- *A* is the address of an array descriptor.
- *X*\$, *Y*\$, *Z*\$ are **STRINGS**.

9.6.1 Miscellaneous Instructions

Name	OpCode	Param	Description
NOP	00		No operation
ADDSP	01	<i>scDelta</i>	SP += <i>scDelta</i> . If <i>scDelta</i> > 0, 'pushed' bytes are initialised to zero.
DUP	02	<i>ucLen</i>	Push the top <i>ucLen</i> stack bytes
COMPL	03		Pop <i>slY</i> ; pop <i>slX</i> ; compare ; push for WORD comparison
RAND	04		Push a LONG random number
ERROR	05	<i>ucError</i>	Generate a P-Code error condition
SYSTEM	06	<i>ucSysCode</i>	Operating system call – see 9.7 The SYSTEM Instruction .

9.6.2 Data Conversion Instructions

Name	OpCode	Description
CVTCW	07	Pop <i>ucX</i> ; <i>swY</i> = <i>ucX</i> ; push <i>swY</i>
CVTWC	08	Pop <i>swX</i> ; <i>ucY</i> = <i>swX</i> ; push <i>ucY</i>
CVTWL	09	Pop <i>swX</i> ; <i>slY</i> = <i>swX</i> ; push <i>slY</i>
CVTLW	0A	Pop <i>slX</i> ; <i>swY</i> = <i>slX</i> ; push <i>swY</i>

9.6.3 Data Access Instructions (*Push and Pop*)

Name	OpCode	Param	Description
PUCCB	0B	<i>ucConst</i>	Push constant CHAR <i>ucConst</i>
PUCWB	0C	<i>scConst</i>	Push constant <i>scConst</i> sign-extended to WORD
PUCWC	0D	<i>ucConst</i>	Push constant <i>ucConst</i> zero-extended to WORD
PUCWW	0E	<i>swConst</i>	Push constant WORD <i>swConst</i>
PURCB	0F	<i>ucAddr</i>	Push CHAR at address <i>ucAddr</i>
PURWB	10	<i>ucAddr</i>	Push WORD at address <i>ucAddr</i>
PURLB	11	<i>ucAddr</i>	Push LONG at address <i>ucAddr</i>
PURSB	12	<i>ucAddr</i>	Push STRING at address <i>ucAddr</i>
PUECW	13	<i>uwAddr</i>	Push CHAR at address <i>uwAddr</i>
PUEWW	14	<i>uwAddr</i>	Push WORD at address <i>uwAddr</i>
PUELW	15	<i>uwAddr</i>	Push LONG at address <i>uwAddr</i>
PUESW	16	<i>uwAddr</i>	Push STRING at address <i>uwAddr</i>
PUFCB	17	<i>scAddr</i>	Push CHAR at address FP + <i>scAddr</i>
PUFWB	18	<i>scAddr</i>	Push WORD at address FP + <i>scAddr</i>
PUFLB	19	<i>scAddr</i>	Push LONG at address FP + <i>scAddr</i>
PUFSB	1A	<i>scAddr</i>	Push STRING at address FP + <i>scAddr</i>
PUFAB	1B	<i>scAddr</i>	Push FP + <i>scAddr</i> as WORD
PUSAB	1C	<i>ucAddr</i>	Push SP – <i>ucAddr</i> as WORD
PUPSB	1D	<i>scAddr</i>	Push 3-byte STRING parameter at address FP + <i>scAddr</i>
PUINC	1E		Pop <i>uwAddr</i> ; push CHAR at address <i>uwAddr</i>
PUINW	1F		Pop <i>uwAddr</i> ; push WORD at address <i>uwAddr</i>
PUINL	20		Pop <i>uwAddr</i> ; push LONG at address <i>uwAddr</i>
PORCB	21	<i>ucAddr</i>	Pop CHAR at address <i>ucAddr</i>
PORWB	22	<i>ucAddr</i>	Pop WORD at address <i>ucAddr</i>
PORLB	23	<i>ucAddr</i>	Pop LONG at address <i>ucAddr</i>
POECW	24	<i>uwAddr</i>	Pop CHAR at address <i>uwAddr</i>
POEWW	25	<i>uwAddr</i>	Pop WORD at address <i>uwAddr</i>
POELW	26	<i>uwAddr</i>	Pop LONG at address <i>uwAddr</i>
POFCB	27	<i>scAddr</i>	Pop CHAR at address FP + <i>scAddr</i>
POFWB	28	<i>scAddr</i>	Pop WORD at address FP + <i>scAddr</i>
POFLB	29	<i>scAddr</i>	Pop LONG at address FP + <i>scAddr</i>
POINC	2A		Pop <i>uwAddr</i> ; pop CHAR at address <i>uwAddr</i>
POINW	2B		Pop <i>uwAddr</i> ; pop WORD at address <i>uwAddr</i>
POINL	2C		Pop <i>uwAddr</i> ; pop LONG at address <i>uwAddr</i>

9. The ZC-Basic Virtual Machine

9.6.4 Integer Arithmetic Instructions

Name	OpCode	Description
ADDW	2D	Pop <i>swY</i> ; pop <i>swX</i> ; push <i>swX</i> + <i>swY</i>
ADDL	2E	Pop <i>slY</i> ; pop <i>slX</i> ; push <i>slX</i> + <i>slY</i>
SUBW	2F	Pop <i>swY</i> ; pop <i>swX</i> ; push <i>swX</i> – <i>swY</i>
SUBL	30	Pop <i>slY</i> ; pop <i>slX</i> ; push <i>slX</i> – <i>slY</i>
MULW	31	Pop <i>swY</i> ; pop <i>swX</i> ; push <i>swX</i> * <i>swY</i>
MULL	32	Pop <i>slY</i> ; pop <i>slX</i> ; push <i>slX</i> * <i>slY</i>
DIVW	33	Pop <i>swY</i> ; pop <i>swX</i> ; push <i>swX</i> / <i>swY</i>
DIVL	34	Pop <i>slY</i> ; pop <i>slX</i> ; push <i>slX</i> / <i>slY</i>
MODW	35	Pop <i>swY</i> ; pop <i>swX</i> ; push <i>swX</i> Mod <i>swY</i>
MODL	36	Pop <i>slY</i> ; pop <i>slX</i> ; push <i>slX</i> Mod <i>slY</i>
ANDW	37	Pop <i>uwY</i> ; pop <i>uwX</i> ; push <i>uwX</i> And <i>uwY</i>
ANDL	38	Pop <i>ulY</i> ; pop <i>ulX</i> ; push <i>ulX</i> And <i>ulY</i>
ORW	39	Pop <i>uwY</i> ; pop <i>uwX</i> ; push <i>uwX</i> Or <i>uwY</i>
ORL	3A	Pop <i>ulY</i> ; pop <i>ulX</i> ; push <i>ulX</i> Or <i>ulY</i>
XORW	3B	Pop <i>uwY</i> ; pop <i>uwX</i> ; push <i>uwX</i> Xor <i>uwY</i>
XORL	3C	Pop <i>ulY</i> ; pop <i>ulX</i> ; push <i>ulX</i> Xor <i>ulY</i>
NEGW	3D	Pop <i>swX</i> ; push – <i>swX</i>
NEGL	3E	Pop <i>slX</i> ; push – <i>slX</i>
ABSW	3F	Pop <i>swX</i> ; push Abs (<i>swX</i>)
ABSL	40	Pop <i>slX</i> ; push Abs (<i>slX</i>)
INCW	41	Pop <i>swX</i> ; push <i>swX</i> + 1
INCL	42	Pop <i>slX</i> ; push <i>slX</i> + 1
NOTW	43	Pop <i>uwX</i> ; push Not (<i>uwX</i>)
NOTL	44	Pop <i>ulX</i> ; push Not (<i>ulX</i>)

9.6.5 Program Control Instructions

(In the **ENTER** and **LEAVE** instructions, F denotes the size of the FP register: 1 in the BasicCard, 2 in the Terminal.)

Name	OpCode	Param	Description
CALL	45	$uwAddr$	Procedure call or GoSub : push PC +3 as WORD ; PC = $uwAddr$
ENTER	46	$ucFrmSiz$	Push FP ; push SP + $ucFrmSiz + F$; FP = SP ; SP = SP + $ucFrmSiz$
LEAVE	47		Return from procedure: SP = FP - F ; pop FP ; pop PC
RETURN	48		Return from GoSub : pop PC
JUMPB	49	$scDisp$	PC = PC + $scDisp + 2$
JUMPW	4A	$uwAddr$	PC = $uwAddr$
JZRWB	4B	$scDisp$	Pop swX ; if $swX = 0$ then PC = PC + $scDisp + 2$
JNZWB	4C	$scDisp$	Pop swX ; if $swX \neq 0$ then PC = PC + $scDisp + 2$
JEQWB	4D	$scDisp$	Pop swY ; pop swX ; if $swX = swY$ then PC = PC + $scDisp + 2$
JNEWB	4E	$scDisp$	Pop swY ; pop swX ; if $swX \neq swY$ then PC = PC + $scDisp + 2$
JLEWB	4F	$scDisp$	Pop swY ; pop swX ; if $swX \leq swY$ then PC = PC + $scDisp + 2$
JGTWB	50	$scDisp$	Pop swY ; pop swX ; if $swX > swY$ then PC = PC + $scDisp + 2$
JGEWB	51	$scDisp$	Pop swY ; pop swX ; if $swX \geq swY$ then PC = PC + $scDisp + 2$
JLTWB	52	$scDisp$	Pop swY ; pop swX ; if $swX < swY$ then PC = PC + $scDisp + 2$
LOOP	53	$scDisp$	Pop swX ; if $swX \geq 0$ then execute JLEWB else execute JGEWB
EXIT	54		Exit the Virtual Machine

9.6.6 Array Instructions

Name	OpCode	Param	Description
ARRAY	55		Pop A ; pop subscript $swIr$ for each dimension r , in reverse order ; push address of array element A ($swI1, swI2, \dots, swIn$)
CHKDIM	56	$ucNdims$	Pop A ; push A ; if $\text{Dim}(A) \neq ucNdims$ then execute ERROR 0C
ALLOCA	57		Pop A ; pop bounds word $uwBr$ for each dimension r , in reverse order; allocate data area of A and initialise all elements to 0
FREEA	58		Pop A ; if Dynamic then deallocate A , else set all elements of A to 0
FREEA\$	59		Pop string array A ; free all strings in A ; if Dynamic then deallocate A
BOUND A	5A		Pop $swHi$; pop $swLo$; push $400 * swLo + (swHi - swLo)$ as WORD
LBOUND	5B		Pop A ; pop $ucDim$; push lower bound of subscript $ucDim$ as WORD
UBOUND	5C		Pop A ; pop $ucDim$; push upper bound of subscript $ucDim$ as WORD

9. The ZC-Basic Virtual Machine

9.6.7 String Instructions

Name	OpCode	Description
COPY\$	5D	Pop $X\$$; pop $Y\$$; $X\$ = Y\$$
FREE\$	5E	Pop 2-byte handle to variable-length string $X\$$; $X\$ =$ empty string
ADD\$	5F	Pop $X\$$; pop $Z\$$; pop $Y\$$; $X\$ = Y\$ + Z\$$
MID\$	60	Pop $swLen$; pop $swStart$; pop $X\$$; push Mid \$($X\$$, $swStart$, $swLen$)
LEFT\$	61	Pop $swLen$; pop $X\$$; push Left \$($X\$$, $swLen$)
RIGHT\$	62	Pop $swLen$; pop $X\$$; push Right \$($X\$$, $swLen$)
LTRIM\$	63	Pop $X\$$; push LTrim \$($X\$$)
RTRIM\$	64	Pop $X\$$; push RTrim \$($X\$$)
UCASE\$	65	Pop $X\$$; pop $Y\$$; $X\$ = \text{UCASE}\$(Y\$)$
LCASE\$	66	Pop $X\$$; pop $Y\$$; $X\$ = \text{LCASE}\$(Y\$)$
STRING\$	67	Pop $X\$$; pop $ucChar$; pop $swLen$; $X\$ = \text{String}\$(swLen, ucChar)$
STRL\$	68	Pop $X\$$; pop slX ; $X\$ = \text{Str}\(slX)
HEX\$	69	Pop $X\$$; pop slX ; $X\$ = \text{Hex}\(slX)
ASC\$	6A	Pop $X\$$; push Asc ($X\$$) as CHAR
LEN\$	6B	Pop $X\$$; push Len ($X\$$) as CHAR
COMP\$	6C	Pop $Y\$$; pop $X\$$; compare ; push for WORD comparison
VALL\$	6D	Pop $X\$$; $slVal = \text{Val}\&(\mathbf{X}\$, ucLen)$; push $slVal$; push $ucLen$
VALHL\$	6E	Pop $X\$$; $slVal = \text{ValH}(\mathbf{X}\$, ucLen)$; push $slVal$; push $ucLen$

9.6.8 Data Initialisation Instructions

Name	OpCode	Params	Description
RDATA	6F	$ucAddr, ucLen, data$	Copy $data$ ($ucLen$ bytes) to address $ucAddr$
FDATA	70	$scAddr, ucLen, data$	Copy $data$ ($ucLen$ bytes) to address FP + $scAddr$

9.6.9 Floating-Point Instructions

Note: These instructions are not implemented in the Compact BasicCard.

Name	OpCode	Description
COMPR	71	Pop rY ; pop rX ; compare ; push for WORD comparison
CVTWR	72	Pop swX ; push swX as REAL
CVTRW	73	Pop rX ; push rX as WORD
CVTLR	74	Pop slX ; push slX as REAL
CVTRL	75	Pop rX ; push rX as LONG
ADDR	76	Pop rY ; pop rX ; push $rX + rY$
SUBR	77	Pop rY ; pop rX ; push $rX - rY$
MULR	78	Pop rY ; pop rX ; push $rX * rY$
DIVR	79	Pop rY ; pop rX ; push rX / rY
NEGR	7A	Pop rX ; push $-rX$
ABSR	7B	Pop rX ; push Abs (rX)
SQRTR	7C	Pop rX ; push Sqrt (rX)
STRR\$	7D	Pop $X\$$; pop rX ; $X\$ = \text{Str}\(rX)
VALR\$	7E	Pop $X\$$; $rVal = \text{Val}\!(X\$, ucLen)$; push $rVal$; push $ucLen$

9.6.10 The XMIT Command Call Instruction

Note: This instruction is available only in a Terminal program.

Name	OpCode	Params	Description
XMIT	7F	$ucType, ucLen$	Send command and process response

Before this instruction is executed, a command must be pushed onto the P-Code stack:

CLA	INS	P1	P2	Lc	IDATA padded to $ucLen$ bytes	Le
------------	------------	-----------	-----------	-----------	--------------------------------------	-----------

Then the command is transmitted according to $ucType$, as follows:

$ucType$	
0	Send Lc bytes in IDATA (no Le)
1	Send Lc bytes in IDATA , followed by Le
2	The top 3 bytes of the IDATA field contain a variable-length string parameter $X\$$. Send $ucLen - 3$ bytes in IDATA , followed by $X\$$.
3	The same as $ucType = 2$, with Le appended to IDATA .
4	The top 3 bytes of the IDATA field contain a variable-length string parameter $X\$$. Send up to Lc bytes of ($ucLen - 3$ bytes followed by $X\$$).
5	The same as $ucType = 4$, with Le appended to IDATA .
7	The same as $ucType = 3$, but $X\$$ was passed ByVal .
9	The same as $ucType = 5$, but $X\$$ was passed ByVal .

9. The ZC-Basic Virtual Machine

9.6.11 Abbreviated Instructions

Instructions from **80** to **FF** are single-byte abbreviations of 2-byte **PUF_xB** / **POF_xB** instructions. For example, **PUFLF1** (instruction **A6**) is an abbreviation of **PUFLB F1**.

Name	OpCode	Description
PUFWED – PUFWFC	80-8F	Push WORD at address FP – (93 – OpCode)
PUFW00 – PUFW0F	90-9F	Push WORD at address FP + (OpCode – 90)
PUFLEB – PUFLFA	A0-AF	Push LONG at address FP – (B5 – OpCode)
PUFL00 – PUFL0F	B0-BF	Push LONG at address FP + (OpCode – B0)
POFWED – POFWFC	C0-CF	Pop WORD at address FP – (D3 – OpCode)
POFW00 – POFW0F	D0-DF	Pop WORD at address FP + (OpCode – D0)
POFLEB – POFLFA	E0-EF	Pop LONG at address FP – (F5 – OpCode)
POFL00 – POFL0F	F0-FF	Pop LONG at address FP + (OpCode – F0)

9.7 The SYSTEM Instruction

The **SYSTEM** P-Code instruction (OpCode **06**) calls an operating system function, according to the first parameter, *SysCode*.

9.7.1 SYSTEM Functions in the Compact BasicCard

The Compact BasicCard has just three **SYSTEM** functions:

OpCode	SysCode	Name	
06	00	WTX	Send a Waiting Time Extension request
06	01	CommandString	Convert a command parameter to a variable-length string
06	02	ResponseString	Convert a variable-length string to a response parameter

9.7.2 SYSTEM Functions in Later BasicCards

The Enhanced and Professional BasicCards have five **SYSTEM** functions with *SysCode* < **80**:

OpCode	SysCode	Name	
06	00	WTX	Send a Waiting Time Extension request
06	03	EnableKey	Enable or disable a cryptographic key or its error counter
06	40	Certificate	Calculate a cryptographic certificate
06	41	DES	DES block encryption primitives
06	55	Key	Built-in Key() function

In addition, these BasicCards support the **FILE SYSTEM** functions – see **9.7.4 FILE SYSTEM Functions**. Professional BasicCards also support some subset of the Plug-In Library procedures – see **9.7.5 Plug-In Library Procedures**.

9.7.3 SYSTEM Functions in the Terminal

<i>OpCode</i>	<i>SysCode</i>	<i>Name</i>	
06	00	WTX	Give the card more time
06	40	Certificate	Calculate a cryptographic certificate
06	41	DES	Des block encryption primitives
06	42	Cls	Clear the screen
06	43	UpdateScreen	Update the screen
06	44	InKey\$	Check for keyboard input
06	45	CardReader	Look for a card reader
06	46	CardInReader	Check whether a card is in the reader
06	47	ResetCard	Reset the card in the card reader
06	48	WriteEeprom	Write EEPROM data back to the image file
06	49	KeyFile	Load a key file
06	4A	EnableEncrypt	Enable auto-encryption (the default)
06	4B	DisableEncrypt	Disable auto-encryption
06	4C	EnableOvCheck	Enable overflow checking (the default)
06	4D	DisableOvCheck	Disable overflow checking
06	4E	Time\$	Date and time as e.g. "Wed Jun 20 15:50:35 1998"
06	4F	ChDrive	Change the current disk drive
06	50	CurDrive	Retrieve the current disk drive
06	51	LongSeed	Seed the random number generator with a LONG value
06	52	StringSeed	Seed the random number generator with a STRING
06	53	OpenLogFile	Start logging of I/O to file
06	54	CloseLogFile	End logging of I/O to file

In addition, the Terminal supports the **FILE SYSTEM** functions listed in the next section.

9.7.4 FILE SYSTEM Functions

The file system functionality in the Terminal and the Enhanced BasicCard is implemented through the **SYSTEM** P-Code instruction. Such **FILE SYSTEM** commands all have **80** <= *SysCode* <= **BF**:

<i>OpCode</i>	<i>SysCode</i>	<i>Name</i>	
06	80	MkDir	Create a directory
06	81	RmDir	Delete a directory
06	82	ChDir	Change the current directory
06	83	CurDir	Retrieve the current directory
06	84	DirCount	Count the filenames that match a wild-card spec
06	85	DirFile	Return the <i>n</i> th matching filename
06	86	EraseFile	Delete a data file
06	87	RenameFile	Rename or move a file or directory

9. The ZC-Basic Virtual Machine

OpCode SysCode Name

06	88	OpenFile	Open a file
06	89	OpenFreeFile	Open a file after finding a free file slot for it
06	8A	CloseFile	Close a file
06	8B	CloseAll	Close all files
06	8C	FreeFile	Find a free file slot
06	8D	FileLength	Return the length of an open file
06	8E	GetFilepos	Return the read/write pointer of an open file
06	8F	SetFilepos	Set the read/write pointer of an open file
06	90	EOF	Return True if at the end of an open file
06	91	Get	Read from a binary file
06	92	GetPos	Get after setting the read/write pointer
06	93	Put	Write to a binary file
06	94	PutPos	Put after setting the read/write pointer
06	95	StartInput	Set the counter of matched input items to 0
06	96	EndInput	Return the counter of matched input items
06	97	Read	Read a specified number of bytes from a sequential file
06	98	ReadLong	Read a formatted LONG value from a sequential file
06	99	ReadSingle	Read a formatted SINGLE value from a sequential file
06	9A	ReadString	Read a formatted STRING from a sequential file
06	9B	ReadBlock	Read a formatted fixed-size block from a sequential file
06	9C	ReadLine	Read a line from a sequential file
06	9D	WriteLong	Write a formatted LONG value to a sequential file
06	9E	WriteSingle	Write a formatted SINGLE value to a sequential file
06	9F	WriteString	Write a formatted STRING to a sequential file
06	A0	PrintLong	Write an ASCII LONG value to a sequential file
06	A1	PrintSingle	Write an ASCII SINGLE value to a sequential file
06	A2	PrintString	Write an ASCII STRING to a sequential file
06	A3	PrintSpaces	Write a specified number of spaces to a sequential file
06	A4	PrintTab	Advance to the next 14-character output field
06	A5	SetColumn	Advance to a specified output column
06	A6	PrintNewLine	Print a new-line character
06	A7	LockFile	Set the access conditions on a file or directory
06	A8	GetLocks	Retrieve the access conditions on a file or directory
06	A9	GetAttr	Retrieve the attributes of a file or directory
06	AA	SetAttr	Set the attributes of a file or directory (Terminal only)

9.7.5 *Plug-In Library Procedures*

Values of *SysCode* between **CO** and **FF** are reserved for Plug-In Library procedures – see **3.13.2 Plug-In Library Procedures**. For details of which codes are assigned to which procedures, see the individual *Library.DEF* files supplied with ZeitControl's development software.

10. Output File Formats

This chapter describes the formats of the various output files generated by the ZC-Basic compiler:

- Image file: program and data in binary format, for use by **ZCMSIM** and **BCLOAD** programs.
- Debug file: symbolic debugging information, for the **ZCMDTERM** and **ZCMDCARD** debuggers.
- List file: source program, compiled P-Code, and data in human-readable text format.
- Map file: the addresses of all symbols in the program, ordered by name and by location.

Note: Throughout this chapter, **bold** numbers are hexadecimal.

10.1 ZeitControl Image File Format

Debug and Image files consist of Sections, each of which starts with a 4-byte ASCII name, followed by a 4-byte section length. Sections are guaranteed to occur in the following order:

For a BasicCard program:

'ZCIF'	Signature Section – “ZeitControl Image File”
'VERS'	Version Section – File format version
'VMTP'	Virtual Machine Type Section – target machine
'CONF'	Configuration File Section (Professional BasicCard only)
'EEPR'	EEPROM Image Section – EEPSYS , CMDTAB , PCODE , STRCON , KEYTAB , EEPDATA , and EEPHEAP regions
'LOAD'	Program Load Section, containing the commands to download to the BasicCard
'CERT'	Code Certification Section (certain Enhanced BasicCard versions)

For a Terminal program:

'ZCIF'	Signature Section – “ZeitControl Image File”
'VERS'	Version Section – File format version
'VMTP'	Virtual Machine Type Section – target machine
'CODE'	P-Code Section – Contents of PCODE region
'DATA'	Data Section – RAMSYS , STRCON , RAMDATA , and RAMHEAP regions
'EEPR'	EEPROM Image Section – EEPDATA and EEPHEAP regions

Numerical 2-byte and 4-byte fields are stored lsb to msb, Intel-style (or Little-Endian). This is in contrast to the Virtual Machine, which is Big-Endian.

Some sections contain string tables. A string table consists of consecutive null-terminated strings. Whenever a name occurs in a Section field, it is to be interpreted as an offset into the string table of the current Section.

10.1.1 Signature Section

Length

4	'ZCIF' (“ZeitControl Image File”)
4	Total length of all remaining sections (= file length – 8)

10.1.2 Version Section

Length

4	'VERS'
4	Section length = 04
1	Major version of software that created this file

1	Minor version of software that created this file
1	Major version of oldest software compatible with this file
1	Minor version of oldest software compatible with this file

10.1.3 Virtual Machine Type Section

Length

4	'VMTP'
4	Section length <i>len</i>
<i>len</i>	<i>MachineType</i>

If *len* = 2, the first byte of *MachineType* is as follows:

00	Terminal
01	Compact BasicCard
02	Enhanced BasicCard

and the second byte is the Machine Sub-type (**00** for Terminal, **01** for Compact BasicCard, various values for Enhanced BasicCard).

If *len* > 2, the Image File contains a Professional BasicCard program, and *MachineType* is an ASCII string containing the version ID of the card.

10.1.4 Configuration File Section (Professional BasicCard only)

Length

4	'CONF'
4	Section length <i>len</i>
<i>len</i>	Full path name of .ZCF BasicCard Configuration File

10.1.5 P-Code Section (Terminal only)

Length

4	'CODE'
4	Section length <i>len</i>
2	Program entry point
<i>len</i> -2	P-Code. The P-Code in the Terminal starts at address 0000 .

10.1.6 Data Section (Terminal only)

Length

4	'DATA'
4	Section length
2	Start address of RAM data
2	Length of RAM data
2	Number of records <i>n</i>
2	Start address of record 0
2	Length <i>len</i> ₀ of record 0
<i>len</i> ₀	Contents of record 0
...	

10. Output File Formats

2	Start address of record $n - 1$
2	Length len_{n-1} of record $n - 1$
len_{n-1}	Contents of record $n - 1$

All RAM bytes not contained in a record must be initialised to **00**.

The Data Section contains the **RAMSYS**, **STRCON**, **RAMDATA**, and **RAMHEAP** regions.

10.1.7 EEPROM Image Section

<i>Length</i>	
4	'EEPR'
4	Section length
2	Start address of EEPROM data
2	Length of EEPROM data
2	Number of records n
2	Start address of record 0
2	Length len_0 of record 0
len_0	Contents of record 0
...	
2	Start address of record $n - 1$
2	Length len_{n-1} of record $n - 1$
len_{n-1}	Contents of record $n - 1$

All EEPROM bytes not contained in a record must be initialised to **FF**.

In the Terminal, the EEPROM Image Section contains just the **EEPDATA** and **EEPHEAP** regions. In the BasicCard, it contains the **EEPSYS**, **CMDTAB**, **PCODE**, **STRCON**, **KEYTAB**, **EEPDATA**, and **EEPHEAP** regions.

10.1.8 Program Load Section (BasicCard only)

<i>Length</i>	
4	'LOAD'
4	Section length
1	State of BasicCard after download (from #State directive or -S parameter)
2	Number n_{WE} of WRITE EEPROM commands
2	Number n_{CRC} of EEPROM CRC commands
2	Address of WRITE EEPROM command 0
1	Length len_0 of WRITE EEPROM command 0
len_0	Contents of WRITE EEPROM command 0
...	
2	Address of WRITE EEPROM command $n_{WE} - 1$
1	Length len_{n-1} of WRITE EEPROM command $n_{WE} - 1$
len_{n-1}	Contents of WRITE EEPROM command $n_{WE} - 1$
2	Address of EEPROM CRC command 0

2	Length of EEPROM CRC command 0
2	CRC of EEPROM CRC command 0
...	
2	Address of EEPROM CRC command $n_{CRC} - 1$
2	Length of EEPROM CRC command $n_{CRC} - 1$
2	CRC of EEPROM CRC command $n_{CRC} - 1$

10.1.9 Code Certification Section

This Section is only required for Enhanced BasicCards **ZC3.1**, **ZC3.2**, and **ZC3.31**.

Length

4	'CERT'
4	Section length len
2	Start address of Certified Code
$len-2$	Code Certificate, to be sent in the SET STATE command

10.2 ZeitControl Debug File Format

A debug file has the same format as an image file, with additional sections containing debug information. The Signature Section has a different name:

'ZCDF' Signature Section – “ZeitControl Debug File”

The debug information sections occur immediately after the **'VMTP'** Virtual Machine Type Section:

'FILE' Files Section – Names of all source files
'TYPE' Types Section – Descriptions of all data types used in the program
'SYMB' Symbols Sections – Labels and variables, one Section for each scope
'LINE' Line Numbers Section – Source line number information
'FIXU' Fixups Section – Cross-references

10.2.1 Signature Section

Length

4	'ZCDF' (“ZeitControl Debug File”)
4	Total length of all remaining sections (= file length – 8)

10.2.2 Files Section

This section contains the names and timestamps of all the source files in the program:

Length

4	'FILE'
4	Section length
2	String table length len_{ST}
len_{ST}	String table
2	Number of files n
2	Name of file 0
4	Number of lines in file 0
2	Length of longest line in file 0

10. Output File Formats

4	Timestamp of file 0
...	
2	Name of file $n - 1$
4	Number of lines in file $n - 1$
2	Length of longest line in file $n - 1$
4	Timestamp of file $n - 1$

10.2.3 Types Section

This section contains definitions of every data type that occurs in the program.

Length

4	'TYPE'
4	Section length
2	String table length len_{ST}
len_{ST}	String table
2	Number of type entries n
7	Type 0
...	
7	Type $n - 1$

Type format (shaded bytes are zero):

Byte	0						
Integer	1						
Long	2						
Single	3						
String	4						
String*n	5	n					
Array	6	<i>ElementType</i>		<i>nDims</i>			
UserType	7	<i>TypeName</i>		<i>nMembers</i>			
Member	8	<i>MemberName</i>		<i>MemberType</i>		<i>Offset</i>	

ElementType, MemberType

Indices of types in the Types section

TypeName, MemberName

Offsets in the string table

nDims

Number of dimensions of the array

nMembers

Number of members in the user-defined type

Offset

Offset of the member in its user-defined type *UserType*

A *UserType* entry is immediately followed by *nMembers* type entries of type *Member*.

10.2.4 Symbols Sections

The first Symbols Section contains global symbols. Each subsequent Symbols Section contains the local symbols for a single procedure. Symbols are sorted by name (according to the 'C' library function `strcmp`). Symbols beginning with '\$' are compiler-generated names.

<i>Length</i>	
4	'SYMB'
4	Section length
2	Procedure start address (0000 for the global Symbols Section)
2	Procedure end address (0000 for the global Symbols Section)
2	String table length len_{ST}
len_{ST}	String table
2	Number of symbols n
8	Symbol 0
...	
8	Symbol $n - 1$

Symbol format (shaded bytes are zero):

Const Long	0	<i>SymbolName</i>	4-byte integer		
Const Single	1	<i>SymbolName</i>	4-byte floating-point number		
Const String	2	<i>SymbolName</i>	<i>String</i>	<i>Len</i>	
<i>Label</i>	3	<i>SymbolName</i>	Address		
<i>Variable</i>	4	<i>SymbolName</i>	Address	<i>Type</i>	<i>Storage</i>
<i>Library Proc</i>	5	<i>SymbolName</i>	<i>Code</i>	<i>Subcode</i>	
Command	6	<i>SymbolName</i>	Address	CLA	INS

SymbolName, String 2-byte offsets in the string table

Type Index in the Types section

Storage **0** = 2-byte absolute
1 = 1-byte absolute
2 = 1-byte signed, FP-relative (procedure parameters, **Private** data)
3 = indirect 1-byte signed, FP-relative (**String** and array parameters)

Code, Subcode **SYSTEM** code and subcode

10.2.5 Line Numbers Section

Line-number entries are sorted in increasing code address order.

<i>Length</i>	
4	'LINE'
4	Section length
2	Number of line-number entries n
10	Line-number entry 0
...	
10	Line-number entry $n - 1$

Line-number entry format:

Code address (2 bytes)	File number (2 bytes)	Line number (2 bytes)	File position (4 bytes)
------------------------	-----------------------	-----------------------	-------------------------

10. Output File Formats

10.2.6 Fixups Section

This Section contains two tables: Labels and Operands. Entries in the Labels table give the label(s) at a given address. Entries in the Operands table give the operand of a P-Code instruction as a symbol (*Label* or *Variable*).

Length

4	'FIXU'
4	Section length
2	Number of entries in Labels table $nLabs$
6	Label entry 0
...	
6	Label entry $nLabs - 1$
2	Number of entries in Operands table $nOps$
6	Operand entry 0
...	
6	Operand entry $nOps - 1$

Label entries and Operand entries have the same format:

Code address (2 bytes)	Symbols Section (2 bytes)	Index of symbol in Symbols Section (2 bytes)
------------------------	---------------------------	--

10.3 List File Format

The format of the list file is illustrated by means of a small example program:

```
Declare ApplicationID = "Small Example Program"
Eeprom MonthLength(1 To 12) = 1,28,31,30,31,30,31,31,30,31,30,31
Const InvalidMonth = &H6F01
Command &H80 &H00 GetMonthLength (N)
  If N < 1 Or N > 12 Then
    SW1SW2 = InvalidMonth
  Else
    N = MonthLength (N)
  End If
End Command
```

This program was compiled for the Compact BasicCard version ZC1.1, with list file and map file requested:

```
ZCBASIC MONTHLEN -CC1 -OL -OM
```

The list file, **MONTHLEN.LST**:

```
❶ File: MONTHLEN.BAS
  ❷ 1 Declare ApplicationID = "Small Example Program"
❸ $ApplicationID:
  ❹ EEPDATA      8082:  15 53 6D 61 6C 6C 20 45 78 61 6D 70 6C 65 20 50
    EEPDATA      8092:  72 6F 67 72 61 6D
    2 Eeprom MonthLength(1 To 12) = 1,28,31,30,31,30,31,31,30,31,30,31
❺ MonthLength:
    EEPDATA      8098:  80 A0 02 01 04 0B 00 18
MonthLength Data:
    EEPDATA      80A0:  00 01 00 1C 00 1F 00 1E 00 1F 00 1E 00 1F 00 1F
    EEPDATA      80B0:  00 1E 00 1F 00 1E 00 1F
```



```

Const80008000:
    EEPDATA      80B8:  80 00 80 00
    3  Const InvalidMonth = &H6F01
    4  Command &H80 &H00 GetMonthLength (N)
GetMonthLength:
    ⑥  PCODE      ⑦ 804E: ⑧46 00 ⑨ ENTER 00
    CMDTAB      8043: 02 80 00 02 80 4E C0 18 07 80 77
    5      If N < 1 Or N > 12 Then
        PCODE      8050: 8F          PUFWFC (N) ⑩
        PCODE      8051: 0C 01      PUCWB 01
        PCODE      8053: 15 80B8    PUELW Const80008000
        PCODE      8056: 3C          XORL
        PCODE      8057: 52 09      JLTWB $If001
        PCODE      8059: 8F          PUFWFC (N)
        PCODE      805A: 0C 0C      PUCWB 0C
        PCODE      805C: 15 80B8    PUELW Const80008000
        PCODE      805F: 3C          XORL
        PCODE      8060: 4F 06      JLEWB $Else001
    6          SW1SW2 = InvalidMonth
$If001:
    PCODE      8062: 0E 6F01    PUCWW 6F01
    PCODE      8065: 22 45      PORWB SW1SW2
    PCODE      8067: 54          EXIT
    7      Else
    8          N = MonthLength (N)
$Else001:
    PCODE      8068: 8F          PUFWFC (N)
    PCODE      8069: 0E 8098    PUCWW MonthLength
    PCODE      806C: 55          ARRAY
    PCODE      806D: 1F          PUINW
    PCODE      806E: CF          POFWFC (N)
    9      End If
    10 End Command
    PCODE      806F: 54          EXIT
$InitCode:
    PCODE      8070: 46 00      ENTER 00
    PCODE      8072: 6F 80 01  RDATA 80 01
                    FF          FF
    PCODE      8076: 47          LEAVE

```

- ❶ Input filename
- ❷ Source code, with line number
- ❸ Compiler-generated label (begins with '\$')
- ❹ Eeprom data (**EEPDATA** is the name of the region)
- ❺ User-generated label (no initial '\$')
- ❻ P-Code (**PCODE** is the name of the region)
- ❼ Address of P-Code instruction
- ❽ P-Code instruction and operands, in hexadecimal
- ❾ P-Code instruction and operands, in text
- ❿ Implicit operand of abbreviated P-Code instruction, in parentheses

10. Output File Formats

10.4 Map File Format

The map file **MONTHLEN.MAP** from the example program in the previous section, **10.3 List File Format**:

❶ Input file: MONTHLEN.BAS

❷ ===== RAM regions =====

Name	Start	End	Length
----	-----	---	-----
RAMSYS	00	4B	4C
STACK	4C	7F	34
RAMDATA			00
RAMHEAP	80	FF	80

❸ ===== EEPROM regions =====

Name	Start	End	Length
----	-----	---	-----
EEPSYS	8020	8042	0023
CMDTAB	8043	804D	000B
PCODE	804E	8081	0034
STRCON			0000
KEYTAB			0000
EEPDATA	8082	80BB	003A
EEPHEAP	80BC	83FF	0344

❹ ===== Symbols by name =====

Name	Scope	Address	Type
----	-----	-----	-----
Algorithm	Global	23	PUBLIC BYTE
CardMajorVersion	Global		CONST=0001
CardMinorVersion	Global		CONST=0001
CLA	Global	47	PUBLIC BYTE
CompactBasicCard	Global		CONST=0001
Const80008000	GetMonthLength	80B8	EEPROM LONG
False	Global		CONST=0000
GetMonthLength	Global	804E	COMMAND &H80 &H00
INS	Global	48	PUBLIC BYTE
InvalidMonth	Global		CONST=6F01
KeyNumber	Global	40	PUBLIC BYTE
Lc	Global	4B	PUBLIC BYTE
Le	Global	44	PUBLIC BYTE
MonthLength	Global	8098	EEPROM INTEGER ARRAY
MonthLength Data	Global	80A0	ARRAY DATA
N	GetMonthLength	FC	PARAM INTEGER
P1	Global	49	PUBLIC BYTE
P1P2	Global	49	PUBLIC INTEGER
P2	Global	4A	PUBLIC BYTE
PCodeError	Global	41	PUBLIC BYTE
ResponseLength	Global	43	PUBLIC BYTE
SW1	Global	45	PUBLIC BYTE
SW1SW2	Global	45	PUBLIC INTEGER
SW2	Global	46	PUBLIC BYTE
True	Global		CONST=FFFFFFFF

❺ ===== Symbols by location =====

10.4 Map File Format

RAM system data:

Name	Scope	Address	Type
----	-----	-----	----
Algorithm	Global	23	PUBLIC BYTE
KeyNumber	Global	40	PUBLIC BYTE
PCodeError	Global	41	PUBLIC BYTE
ResponseLength	Global	43	PUBLIC BYTE
Le	Global	44	PUBLIC BYTE
SW1	Global	45	PUBLIC BYTE
SW1SW2	Global	45	PUBLIC INTEGER
SW2	Global	46	PUBLIC BYTE
CLA	Global	47	PUBLIC BYTE
INS	Global	48	PUBLIC BYTE
P1	Global	49	PUBLIC BYTE
P1P2	Global	49	PUBLIC INTEGER
P2	Global	4A	PUBLIC BYTE
Lc	Global	4B	PUBLIC BYTE

EEPROM user data:

Name	Scope	Address	Type
----	-----	-----	----
MonthLength	Global	8098	EEPROM INTEGER ARRAY
MonthLength Data	Global	80A0	ARRAY DATA
Const80008000	GetMonthLength	80B8	EEPROM LONG

⑥ User code:

Name	Scope	Address	Type
----	-----	-----	----
GetMonthLength	Global	804E	COMMAND &H80 &H00
Initialisation Code	Global	8070	SUB

⑦ Local variables:

Name	Scope	Address	Type
----	-----	-----	----
N	GetMonthLength	FC	PARAM INTEGER

- ❶ Input filename.
- ❷ RAM regions: The addresses and lengths of the regions in RAM.
- ❸ EEPROM regions: The addresses and lengths of the regions in EEPROM.
- ❹ Symbols by name: All the symbols in alphabetical order.
- ❺ Symbols by location: All the symbols, ordered according to location and address.
- ❻ User code: The addresses of all the procedures and labels in the source program.
- ❼ Local variables: The signed FP-relative addresses of parameters and **Private** data.

Index

A

Abs	37
Access Conditions.....	62
ACos Mathematical Function	99
Advanced Encryption Standard	87, 142
AES Algorithm	142
AES Function	87
AES Library	87
Algorithm	44, 47
Allow9XXX.....	19
Answer To Reset.....	43
Append mode	59
Application ID	43
Array Descriptor Format	49
Array Functions	37
Array Parameters	36
Arrays	22
As type	23
Asc	37
ASin Mathematical Function	99
ASSIGN NAD Command	132
Assignment Statements	27
At address	23
ATan Mathematical Function.....	99
ATan2 Mathematical Function.....	99
ATR	43, 107
ATR Declaration.....	43
Attributes	57
Automatic Encryption.....	47

B

BasicCard.....	8
BasicCard Virtual Machine.....	155
BasicCard-Specific Features	43
BCKEYS.EXE.....	82
BCLOAD.EXE	80
Beep Subroutine	102
BgCol	48
Binary Files.....	61, 62
Binary mode.....	59
Block Waiting Time.....	21, 107
Built-in Commands.....	117
Built-in Functions	37
BWT	21, 107
Byte data type	22

C

Call	35
Card Loader	80
Card State.....	20
CardInReader	45
CardReader	45
Ceil Mathematical Function.....	99
Certificate	38, 41

Certificate Generation	41, 142
ChDir	55
ChDrive	57
Chr\$	37
CLA	32, 34, 44
Class byte	32, 34, 44
CLEAR EEPROM Command.....	122
Close File.....	60
Close Log File	46
Cls	44
Command Calls	35
Command Definition.....	32
Command-response protocol.....	7
COMMANDS.DEF.....	134
Communications.....	45, 106
Compact BasicCard.....	11
ComPort	47
Computed GoTo/GoSub.....	31
Conditional Compilation	19
Cos Mathematical Function	99
CosH Mathematical Function	99
CRC16 Function	101
CRC32 Function	101
Create File	58
CurDir	55
CurDrive	58
Current Disk Drive	57, 58
CursorX	48
CursorY	48
Custom Lock	63

D

Data Declaration.....	23
Data Storage	21
Data Types.....	22
Data Types, P-Code.....	157
Date	46
Debug File Format.....	171
Debug File, Generating	78
Declare ApplicationID	43
Declare ATR	43
Declare Key	39
Declare Polynomials	40
DefByte	48
DefInt	48
DefLng	48
DefSng	48
DefString	48
DefType Statement.....	48
Delete File	58
DES Algorithm.....	137
DES Encryption Primitives	41
Dir	56, 64
Directory Attributes.....	57
Directory Commands	54

Directory Definition.....	64
Directory Names.....	51
Directory-Based File Systems.....	51
Disable Encryption	43, 47
Disable Key	41
Disable OverflowCheck	48
Disk Drive.....	57, 58
Do-Loop.....	30
Dynamic arrays.....	22

E

EC-161 Library.....	92
EC161GenerateKeyPair	94
EC161HashAndSign	94
EC161HashAndVerify	94
EC161SessionKey	95
EC161SetCurve	93
EC161SetPrivateKey	94
EC161SharedSecret	95
EC161Sign	94
EC161Verify	95
EC-167 Library.....	88
EC167GenerateKeyPair	89
EC167HashAndSign	90
EC167HashAndVerify	90
EC167SessionKey	91
EC167SetCurve	89
EC167SetPrivateKey	90
EC167SharedSecret	90
EC167Sign	90
EC167Verify	90
ECHO Command.....	131
EEPROM CRC Command.....	125
Eeprom data.....	21
EEPROM SIZE Command.....	121
Elliptic Curve Library.....	88
Enable Encryption.....	43, 47
Enable Key	40
Enable OverflowCheck	48
Encryption.....	39
Encryption Algorithms.....	137
Encryption Functions.....	38
END ENCRYPTION Command.....	130
Enhanced BasicCard.....	11
EOF	64
Error Counter.....	40
Error Directive.....	20
Error File, Generating.....	78
Error Handling.....	42
Executable Files.....	13
Execute Subroutine.....	101
Exit	28
Exp Mathematical Function.....	99
Expressions.....	25

F

fa... File Attributes.....	57
FastEepromWrites Subroutine.....	102
fe... File System Errors.....	53
FgCol	48

File	65
File Attributes.....	57
File Definition.....	65
File Definition Sections.....	10
FILE IO Command.....	133
File Names.....	51
File System Commands.....	53
File types.....	67
FileError	44, 48
FILEIO.DEF.....	65
Files and Directories.....	51
Fixed arrays.....	22
Floor Mathematical Function.....	99
Folders.....	51
For-Loop.....	29
FreeFile	64
Function Calls.....	35
Function Definition.....	31

G

GET APPLICATION ID Command.....	127
Get Lock	63
GET STATE Command.....	120
GetAttr	57
GetDateTime Subroutine.....	100
GoSub.....	28
GoTo.....	28

H

Hex\$	37
Hexadecimal Constants.....	16
Hypot Mathematical Function.....	99

I

I/O Logging.....	46
I-block (T=1 protocol).....	112
IDEA Library.....	98
IdeaDecrypt	98
IdeaEncrypt	98
If-Then-Else.....	29
Image File Format.....	168
Image File, Generating.....	78
Image Files.....	13
Implementing Encryption.....	39
Initialisation Code.....	9
InKey\$	45
Input	45, 61
Input mode.....	59
INS	32, 34, 44
Installation of Support Software.....	67
Instruction byte.....	32, 34, 44
Integer data type.....	22
Inverse Convention.....	19

K

Key Configuration.....	40
Key Declaration.....	39
Key Error Counter.....	40
Key Generator.....	81
Key Loader.....	82

Keyboard Input	45
KEYGEN.EXE	81
KeyNumber	44, 47
Kill	58

L

Labels.....	28
LBound	37
Lc	44
LCase\$	37
Le	44
Left\$	37
Len (of data)	37
Len (of file)	64
LibError	83
Libraries	83
LIBVER.EXE	83
Line Input	45, 61
List File Format	174
List File, Generating	78
Listing Directives	20
LOAD state.....	117
Lock	63
Lock File	62
Log10 Mathematical Function.....	99
LogE Mathematical Function	99
Long data type	22
LTrim\$	38

M

Map File Format	176
Map File, Generating	78
MATH Library	99
Memory Allocation.....	50
Message Decryption Functions	139, 143
Message Encryption Functions	138, 142
Mid\$	38
MISC Library	100
MkDir	54

N

Name	55
NEW state.....	117
nParams	48
Numerical Expressions	25
Numerical Functions	37

O

Octal Constants	16
Open File.....	58
Open File Slots.....	20
Open Log File	46
Option Base	48
Option Explicit	49
Options.....	18
Output File Formats	168
Output mode	59
Overflow Checking	48

P

P1	44
P1P2	44
P2	44
Param\$	48
Parameter Passing.....	36
Path Names.....	51
pc... P-Code Errors	115
PC/SC Functions	46
P-Code Instructions	158
P-Code Interpreter	79
P-Code Stack	156
PCodeError	44, 48
Permanent Data	11, 14
PERS state	117
PKCS	83
Plug-In Libraries	83
Polynomial Declaration.....	40
Pow Mathematical Function.....	99
Pre-Defined Commands	117
Pre-Defined Constants.....	21
Pre-Defined Files.....	52
Pre-Defined Variables	44, 47
Pre-Processor Directives	18
Print	45, 60
Private data.....	21
Procedure Calls	35
Procedure Definition	31
Procedure Definitions.....	9
Procedure Parameters	36
Processor Cards	6
Professional BasicCard.....	12
Program Layout.....	9
Programming processor card.....	7
Public data	21
Put	61

R

Random Files.....	61, 62
Random mode	59
Random Number Generation.....	42
Randomize	42
RandomString Subroutine	102
READ EEPROM Command.....	124
Read From Files	61
Read Key File	40
Read Lock	62
Read Unlock	62
Read Write Lock	62
Read Write Unlock	62
ReDim	22
Renaming Files.....	55
Reserved words	17
ResetCard	45
ResponseLength	44, 47
Return	28
Right\$	38
Rmdir	54
Rnd	37, 42
RSA Library	83

RsaDecrypt	85
RsaEncrypt	85
RsaGenerateKey	84
RsaOAEPDecrypt	87
RsaOAPEncrypt	87
RsaPKCS1Decrypt	86
RsaPKCS1Encrypt	86
RsaPKCS1Sign	86
RsaPKCS1Verify	86
RsaPseudoPrime	85
RsaPublicKey	85
RTrim\$	38
RUN state	117
Run-Time Memory Allocation.....	157
S	
Save Eeprom Data.....	46
Screen Output	44
Searching for Files	56
Secure Hash Algorithm.....	97
Seek	64
Select Case	30
Sequential Files.....	60, 61
SET STATE Command	126
SetAttr	57
SG-LFSR	145
SG-LFSR with CRC	146
SHA-1 Library	97
ShaAppend	97
ShaEnd	97
ShaHash	97
ShaRandomHash	98
ShaRandomSeed	98
ShaStart	97
Shrinking Generator.....	145
Sin Mathematical Function.....	99
Single data type	22
SinH Mathematical Function.....	99
Sleep Subroutine.....	101
Source File	16
Source File Inclusion	18
Space\$	38
Sqrt	37
Stack Size.....	20
START ENCRYPTION Command.....	128
States of the BasicCard	117
Static data.....	21
Storage Requirements	53
Str\$	38
String data type	22
String Expressions	27
String Functions	37
String Parameter Format	50
String Parameters	36
String\$	38
String*n data type	22
Strings, P-Code	157
Subroutine Calls.....	35
Subroutine Definition.....	31
Support Software	67
SuspendSW1SW2Processing Subroutine..	103
sw... Status Codes.....	114
SW1	44, 114
SW1SW2	44, 48
SW2	44, 114
SYSTEM Instruction	164
T	
T=1 Protocol	112
Tan Mathematical Function	99
TanH Mathematical Function.....	99
Terminal Program.....	13
Terminal Program Layout	13
Terminal Virtual Machine	155
Terminal-Specific Features	44
TEST state	117
Time\$	46
TimeInterval Function	100
Tokens	16
Trim\$	38
U	
UBound	37
UCase\$	38
UnixTime	100
Unlock	63
Unlock File	62
UpdateCRC16 Subroutine	101
UpdateCRC32 Subroutine	101
User-Defined Parameters	37
User-Defined Types	24
V	
Val!	38
Val&	38
ValH	38
Virtual card readers	69
Virtual Machine.....	155
W	
While-Loop	30
Write	60
Write Eeprom	46
WRITE EEPROM Command	123
Write Lock	62
Write to file	60
Write Unlock	62
WTX Request	113
WTX Statement	43, 47
Z	
ZC-Basic Compiler.....	78
ZC-Basic language	16
ZCINC Environment Variable.....	18
ZCMBASIC.EXE.....	78
ZCMDCARD.EXE.....	75
ZCMDTERM.EXE	73
ZCMSIM.EXE	79
ZCPDE.EXE	71
ZCPORT Environment Variable.....	47, 77

