

# BasicCard Support Software Change Log

This document describes the changes in each version of the BasicCard support software since Version 2.50.

## Changes in Version 3.21

### *Interrupted Download*

If the **WBCLOAD** program was interrupted for any reason, the BasicCard would sometimes become unusable. This was a problem in the support software, not the BasicCard itself. It has been fixed in Version 3.21.

## Changes in Version 3.20

### *New BasicCard ZC3.31*

Version 3.20 of the software supports the new BasicCard version ZC3.31.

### *Compiler Fix*

The WZCBASIC compiler sometimes generated an invalid **.DBG** file for a program that contained initialised **Private** arrays. This has been fixed in Version 3.20.

## Changes in Version 3.12

### *Arrays of Fixed-Length Strings*

In certain circumstances, the WZCBASIC compiler was handling arrays of fixed-length strings incorrectly. For example, the statement “**Get #1, , FS(I)**” was generating an internal compiler error when **FS** was an array of fixed-length strings. This has been fixed in Version 3.12.

### *File Length Restrictions in the Built-In Editor*

The built-in editor in the ZeitControl Double Debugger can only be used to edit source files up to 32767 bytes in length. This was always the case, but it has now been made explicit in the documentation.

## Changes in Version 3.11

### *Long Names in Compiler*

Procedure and array names longer than about 40 characters were sometimes causing the WZCBASIC compiler to crash. This has been fixed in Version 3.11: there is now no limit on the lengths of names.

## Changes in Version 3.10

### *New BasicCard Types*

Version 3.10 supports the new BasicCards ZC3.7, ZC3.8, and ZC3.9. These are functionally equivalent to BasicCards ZC3.1, ZC3.2, and ZC3.3 respectively, but run on different hardware.

## ***Compiler Fix***

The WZCBASIC compiler had an obscure bug that sometimes caused it to compile non-constant strings in **Case** statements incorrectly. This has been fixed in Version 3.10.

## **Changes in Version 3.04**

### ***T=1 Protocol Error Recovery***

The T=1 Protocol error recovery mechanism was not working correctly. This could cause cards to become permanently unusable if a protocol error occurred during program download. This has been corrected in Version 3.04.

### ***Pre-Defined Constants***

The pre-defined constants **CardMajorVersion** and **CardminorVersion** are available in BasicCard programs (see 3.3.12 **Pre-Defined Constants**).

### ***DEBIT Example Application***

The example application in the BasicCrd\Examples\Debit directory was not allowing for floating-point rounding. This has been corrected.

## **Changes in Version 3.03**

### ***Series 3 Consolidation***

The Series 3 Enhanced BasicCard required many changes to the software, not all of which were implemented in Versions 3.01 and 3.02. For example, the **WBCKEYS** key-loading program was not compatible with the Series 3 Enhanced BasicCard, and some of the Plug-In Libraries were not updated. These changes have now been implemented in Version 3.03.

### ***Even Faster Elliptic Curves***

New versions of the Enhanced BasicCard are available, with a built-in Elliptic Curve Fast Signature Algorithm (**EC-FSA**)

- Enhanced BasicCard ZC3.5, with 6 kilobytes of user-programmable EEPROM;
- Enhanced BasicCard ZC3.6, with 14 kilobytes of user-programmable EEPROM.

They are based on the same hardware as Enhanced BasicCards ZC3.3 and ZC3.4, respectively; the reduction in EEPROM size is due to the built-in **EC-FSA**. These cards can compute an Elliptic Curve signature in 1.2 seconds (including **T=1** communication overhead). This is twice as fast as previous Enhanced BasicCards.

## **Changes in Version 3.02**

### ***Compiler Fix***

DBG files created by the compiler were not fully compatible with the new Version 3.01 format. This has been fixed in Version 3.02.

# Major Changes in Version 3.01

## Overview

The company that manufactures the BasicCard processor has decided, for security reasons, that it can no longer allow members of the public to download native machine code into EEPROM in any of its products. It does not consider the BasicCard intrinsically insecure, but it has insisted that we close the door on this possibility to reassure its other clients. ZeitControl has reluctantly complied.

Such a possibility is not mentioned in the BasicCard documentation, so some readers may be puzzled by this. However, from the capabilities of our Plug-In Libraries, it is clear to an expert smart-card programmer that we at ZeitControl have ways of running native machine code from EEPROM; and some adventurous programmers have taken these libraries apart to see how we do it. Our attitude at ZeitControl has been: Good luck to them! We have never actively supported such developments, but only because we don't have the resources. Now we have to say: Sorry, but the fun's over. No more native code.

What impact will this have on a typical user? The answer is, no impact at all, beyond the following:

- EEPROM has shrunk by 67 bytes;
- the **WBCLOAD** program takes a little longer to run.

ZeitControl is no longer delivering the Enhanced BasicCards ZC2.3 and ZC2.4, although our software still supports such cards for customers who purchased them prior to Version 3.01. The new cards are the **Enhanced BasicCard ZC3.3** and **Enhanced BasicCard ZC3.4**, and they are functionally identical to the old Enhanced BasicCards – until you try and download your own native code. (We're not going to spoil everybody's fun by describing all the measures we have taken to prevent this!)

## New BasicCard Versions

Versions currently available are the **Enhanced BasicCard ZC3.3**, and the **Enhanced BasicCard ZC3.4**. The **WZCBASIC** command-line compiler options for these cards are **-C3.3** and **-C3.4** respectively. The EEPROM capacities of these cards are 67 bytes short of 8K and 16K respectively.

Where necessary to distinguish between the old and the new Enhanced BasicCards, they will be called the *Series 2* and *Series 3* Enhanced BasicCards.

## Changes to the ZC-Basic Language

- The **Peek** and **Poke** statements have been removed from the language.
- Data declarations of the form

*variable At address*

are only allowed if *variable* is wholly contained in an already declared variable.

## Changes to the Built-In Commands

There is one important change in the built-in command set: the **WRITE EEPROM** command is no longer supported as a user-callable command. If you call this command, you do so at your own risk – the likely result is an unusable card.

## 16-bit DOS Versions No Longer Supported

The 16-bit DOS versions of the support software programs are no longer supported. (This is only an incidental result of the changes – the compiler finally just got too big.) If you need to use these programs, you must stick with the previous software package.

## **WBCKEYS Key Download Program**

This program has not yet been converted to work with the Series 3 Enhanced BasicCard. As far as we know, users have never used this program in earnest, so we are not making this a high priority. If you do need to use this program, let us know, and we will move it up the list.

### **And Now the Good News...**

Version 3.01 comes complete with a new Elliptic Curve Plug-In Library, **EC-161**, that is twice as fast as the old **EC-160** library! An example program is in the BasicCard\Examples\EC-161 directory. The new library uses Elliptic Curves over  $\text{GF}(2^{168})$  instead of  $\text{GF}(2^{162})$ , so it is not compatible with the **EC-160** library. The **EC-160** library is no longer supported, so if you are using the old library and are unable to change to the new library, you must use a previous version of the software.

## **Changes in Version 2.78**

Version 2.77 introduced a bug in reporting the ATR from a simulated BasicCard. This is fixed in Version 2.78.

## **Changes in Version 2.77**

### **If Not...**

In Basic, **Not** is a bitwise operator, not a logical operator. So the code

```
Private X = &H1234 : If Not X Then Print "Not X" : Else Print "Not Not X"
```

prints "Not X" (because **Not X** is equal to **&HEDCB**, which is non-zero). Only if **X** were equal to **-1** would "Not Not X" be printed.

The **ZCBASIC** compiler has been handling this inconsistently, treating **Not** in some circumstances as a logical operator. For instance, the above example would print "Not Not X". This has been fixed in Version 2.77.

**IMPORTANT:** This fix may cause existing programs to behave differently if they contain **If Not...** statements. If in doubt, replace

```
If Not expression Then...
```

with

```
If expression <> 0 Then...
```

### **Multiple Card Readers**

The communications software in the Terminal program Virtual Machine has been re-written to handle multiple card readers simultaneously. Formerly, switching the card reader (by changing the **ComPort** variable) meant that the previous card reader was forgotten. For instance, if you had card readers on serial ports **COM1** and **COM3**, with a BasicCard in each, the following code would report the error **swCardNotReset**:

```
#Include COMMERR.DEF  
  
ComPort = 1 : ResetCard : Call CheckSW1SW2()  
ComPort = 3 : ResetCard : Call CheckSW1SW2()  
ComPort = 1 : Call Echo ("abc") : Call CheckSW1SW2()
```

In Version 2.77, the Virtual Machine remembers that the card reader attached to **COM1** has an active card inserted, so this example works as expected. This lets you conduct conversations between two cards.

## ***CyberMouse Support***

The CyberMouse card reader (serial port version) can now be used without having to install any PC/SC drivers. Just set **ComPort** to the appropriate number (1 through 4 for **COM1** through **COM4**), and the Virtual Machine recognises it automatically. (The USB version of the CyberMouse, however, can only be accessed via PC/SC.)

## **Changes in Version 2.76**

### ***TimeInterval Function***

The **TimeInterval** function in the **MISC** library had a bug that could cause it to be off by one hour. This is fixed in Version 2.76.

## **Changes in Version 2.75**

### ***Font Size in Double Debugger***

The Double Debugger was not coping properly with systems that had no “Courier” font installed. In such systems, the text displayed in the child windows was so small as to border on invisibility. This is fixed in Version 2.75.

## **Changes in Version 2.74**

### ***Command Execution From ZC-Basic***

**MISC** library Version 1.11 contains an **Execute()** subroutine that executes an operating system command line from a Terminal program.

### ***Beep Subroutine***

You can now make a noise from a Terminal program, with the **Beep()** subroutine in **MISC** library Version 1.11.

### ***Card Reinsertion in PC/SC Reader***

If a card was removed from a PC/SC reader and subsequently reinserted, the ZC-Basic interpreter sometimes failed to see the reinsertion. This is fixed in Version 2.74.

## **Changes in Version 2.73**

### ***File Lock Bug in Enhanced BasicCard***

The Enhanced BasicCard 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 single-key read or write lock. To get round this bug, all single-key locks in the Enhanced BasicCard are treated as double-key locks, with a dummy key number 255 as the second key. To make this work, key number 255 is no longer allowed in Enhanced BasicCard programs. Existing programs that use this key number will therefore have to be amended. We apologise for any inconvenience this may cause.

### ***Environment Variables***

The development software recognises two environment variables:

- **ZCPORT** specifies the default value of the card reader COM port;
- **ZCINC** specifies a list of include-file search directories.

To specify an environment variable, use the MS-DOS SET command.

### ***IDEA Plug-In Library***

The new **IDEA** Plug-In Library implements the International Data Encryption Algorithm.

### ***LIBVER.EXE***

The program LIBVER.EXE, in directory BasicCrD\Lib, displays the name and version number of a ZeitControl Plug-In Library file.

### ***More Accurate Time Function***

**MISC** library Version 1.10 contains new functions, giving the time of day to the same resolution as the system clock (Terminal programs only). See ECINIT.BAS and ECTEST.BAS in BasicCrD\Examples\EC for examples.

### ***Improved Elliptic Curve Library***

The **EC-160** Elliptic Curve library Version 1.20 is significantly faster than the previous version. Shared secret derivation is 50% faster (12 seconds instead of 24) and signature generation is 30% faster (4 seconds instead of 6).

### ***Editor Fixed in Double Debugger***

Under certain circumstances, the editor in the Double Debugger was leaving random text at the end of files. This is fixed in Version 2.73.

## **Changes in Version 2.72**

### ***Windows NT with External Chipi Card Reader***

On some fast machines, Windows NT was failing to detect an external Chipi card reader. This has been fixed in Version 2.72.

### ***Elliptic Curve Library***

Version 1.11 of library **EC-160** is included. This fixes a bug in **EC160SharedSecret** in the (real) Enhanced BasicCard, which caused invalid session keys to be generated.

## **Changes in Version 2.71**

This version contains an improved **EC-160** 160-bit Elliptic Curve Cryptography library.

## **Changes in Version 2.70**

### ***Elliptic Curve Cryptography***

Plug-In Library **EC-160** provides 160-bit Elliptic Curve Cryptography routines in Enhanced BasicCard and Terminal programs, as defined in the proposed IEEE standard P1363.

### ***Secure Hash Algorithm***

The **SHA-1** Plug-In Library implements the Secure Hash Algorithm, revision 1, as defined in the Federal Information Processing Standard FIPS-180. The library also includes a cryptographically strong Pseudo-Random Number Generator. (For Enhanced BasicCard and Terminal programs.)

## **Mathematical Functions**

The **MATH** Plug-In Library provides mathematical functions such as **Exp** and **Sin**. (For Terminal programs only.)

## **Plug-In Libraries**

ZCBASIC Compiler Version 2.70 lets you link ZeitControl libraries with your ZC-Basic code using the new **#Library** directive. Three ZeitControl libraries are currently available: **EC-160** (160-bit Elliptic Curve Cryptography), **SHA-1** (Secure Hash Algorithm, revision 1), and **MATH** (mathematical functions).

## **More Flexible Initialisation Code Placement**

Previously, Initialisation Code had to be the first block of executable code in the source file. With Version 2.70, the first block of executable code that is not part of a procedure is assumed to be the Initialisation Code. This has two beneficial effects:

- You don't have to **#Include** a definition file at the start of your program and a source file at the end – procedures can be defined (and not just declared) in the definition files themselves. For example, programs that call `CheckSW1SW2()` just need “**#Include COMMERR.DEF**” at the beginning, and no longer need “**#Include COMMERR.BAS**” at the end.
- You can remove `-I\BasicCrd\Tools` from the compiler options for your Terminal programs.

The only programs that are adversely affected by the change are those that sandwich a ZeitControl definition file between blocks of Initialisation Code. The ZCBASIC Compiler will reject such programs with the error message “Not allowed outside a SUB or FUNCTION” when it reaches the second block of code.

To fix this, simply move the **#Include** statement to before or after the Initialisation Code.

## **#Message Pre-Processor Directive**

The ZCBASIC Compiler recognises a new **#Message** pre-processor directive. This directive prints an informative message to standard error, and continues compilation. See for example `BasicCrd\Tools\CardUtil.Bas`.

## **Image File Format**

The format of a ZeitControl Image File has changed:

- A new ‘**LIBR**’ Libraries Section has been added;
- The ‘**CODE**’ Section in a Terminal program image file begins with an Entry Point address.

## **Changes in Version 2.62**

### **Upgrade 2.3-001**

The Enhanced BasicCard ZC2.3 had a bug that occasionally (very occasionally) caused it to return with the mysterious error code `SW1-SW2=&H6406`: **P-Code Error pcReturnWithoutGoSub**.

As of 13th April 1999, cards delivered by ZeitControl do not have this bug. If you have any cards from an earlier date, you can upgrade them yourself from the `BasicCrd\Upgrades` directory, using program `2_3-001.EXE` (under DOS) or `W2_3-001.EXE` (under Windows 95). Run the program with parameter ‘?’ to get a list of command-line parameters. Note that cards already in state RUN cannot be upgraded.

The program prompts you for confirmation before making any changes to your card. So if you are uncertain, you can use the program simply to check whether your cards already contain this upgrade or not.

This upgrade doesn't slow the card down, or decrease the EEPROM available to the programmer, so you are advised to install it on all your cards.

### ***Open For Append***

The Enhanced BasicCard had a bug that sometimes caused **Open For Append** to fail. This has been fixed in Version 2.62.

### ***Length of Random File***

In **4.10 Miscellaneous File Operations**, the **Len** function was described as follows:

**Len** (#filenum) Returns the length of file *filenum* as a **Long** value (or the number of records if **Access=Random**).

This was never the case, except in Terminal programs. The new (correct) description is:

**Len** (#filenum) Returns the length of file *filenum* in bytes, as a **Long** value.

The Terminal Virtual Machine has been changed to be consistent with the Enhanced BasicCard.

## **Changes in Version 2.61**

### ***PC/SC Time-out Problems***

As noted below (**Changes in Version 2.60**), the PC/SC interface doesn't let the Terminal program extend the time-out period. So the "**WTX n**" statement has no effect in a Terminal program if **Comport** > 4. Version 2.61 of the software solves this problem in two ways:

- **BCLOAD** Version 2.61 splits its **CLEAR EEPROM** and **EEPROM CRC** commands into small chunks when it is dealing with a PC/SC reader, so that no time-outs occur. (The source code for this program can be found in the `BasicCrd\Source\BCLoad` directory.)
- The card reader calculates the default time-out for a card from a field in the card's **ATR** (Answer To Reset – see **6.1 The T=1 Protocol**). The ZC-Basic programmer can now change this field using the **#BWT** pre-processor directive – see **3.3.9 Block Waiting Time**. Note that the new **BWT** value only applies in states **TEST** and **RUN**.

### ***Windows® NT***

In Version 2.60 (but not in earlier versions), executable files generated by the ZC-Basic compiler were rejected as invalid by Windows® NT. This affected not only users' programs, but the ZeitControl programs `WBCLOAD.EXE` and `WBCKEYS.EXE`. This has been fixed in Version 2.61.

### ***Chipi Beeper***

For those of you with an external Chipi card reader: it should only beep once now, instead of four times (or sometimes even six).

### ***Documentation***

The following warning has been added to **6.4.8 The EEPROM CRC Command**:

*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.

### ***Array Elements as Data Items***

The ZC-Basic compiler was incorrectly compiling certain instances of **Put**, **Get**, and **Certificate** statements when the data item was an array element. This is fixed in Version 2.61.

## ***Public and Static Strings***

In an Enhanced BasicCard program, **String** variables declared as **Public** or **Static** were causing the compiler to fail with an internal error if a debug file was requested with the **-OD** command-line parameter. This is fixed in Version 2.61.

## **Changes in Version 2.60**

### ***PC/SC Support***

Version 2.60 supports the PC/SC standard. Any PC/SC-compatible reader can be used with the support software. To access PC/SC reader number  $n$ , set **ComPort** =  $n+100$ . See **3.20.4 PC/SC Functions** for details.

*Note:* The PC/SC interface does not support the functionality described in **3.20.9 Giving the Card More Time**. If you need to use this feature, you must use a ZeitControl Chipi<sup>®</sup> card reader with **ComPort**  $\leq 4$ .

## **Changes in Version 2.52**

### ***STRCON Corruption***

Under certain circumstances, strings in the **STRCON** region were being overwritten while executing a **Mid\$**-type assignment statement. This is fixed in Version 2.52.

## **Changes in Version 2.51**

### ***WTX in Simulated BasicCard***

The WTX statement was generating a Frame Boundary Violation when executed in a simulated BasicCard. This is fixed in Version 2.51.

### ***#If / #Elseif / #Else***

The ZCBASIC pre-processor was incorrectly compiling code after a **#Else** statement in certain cases. This is fixed in Version 2.51.

### ***Documentation***

Some obscurities in **3.16 Encryption** have been clarified. A paragraph has been added to **3.18 Error Handling**.