

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 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® card reader with **ComPort** ≤ 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**.