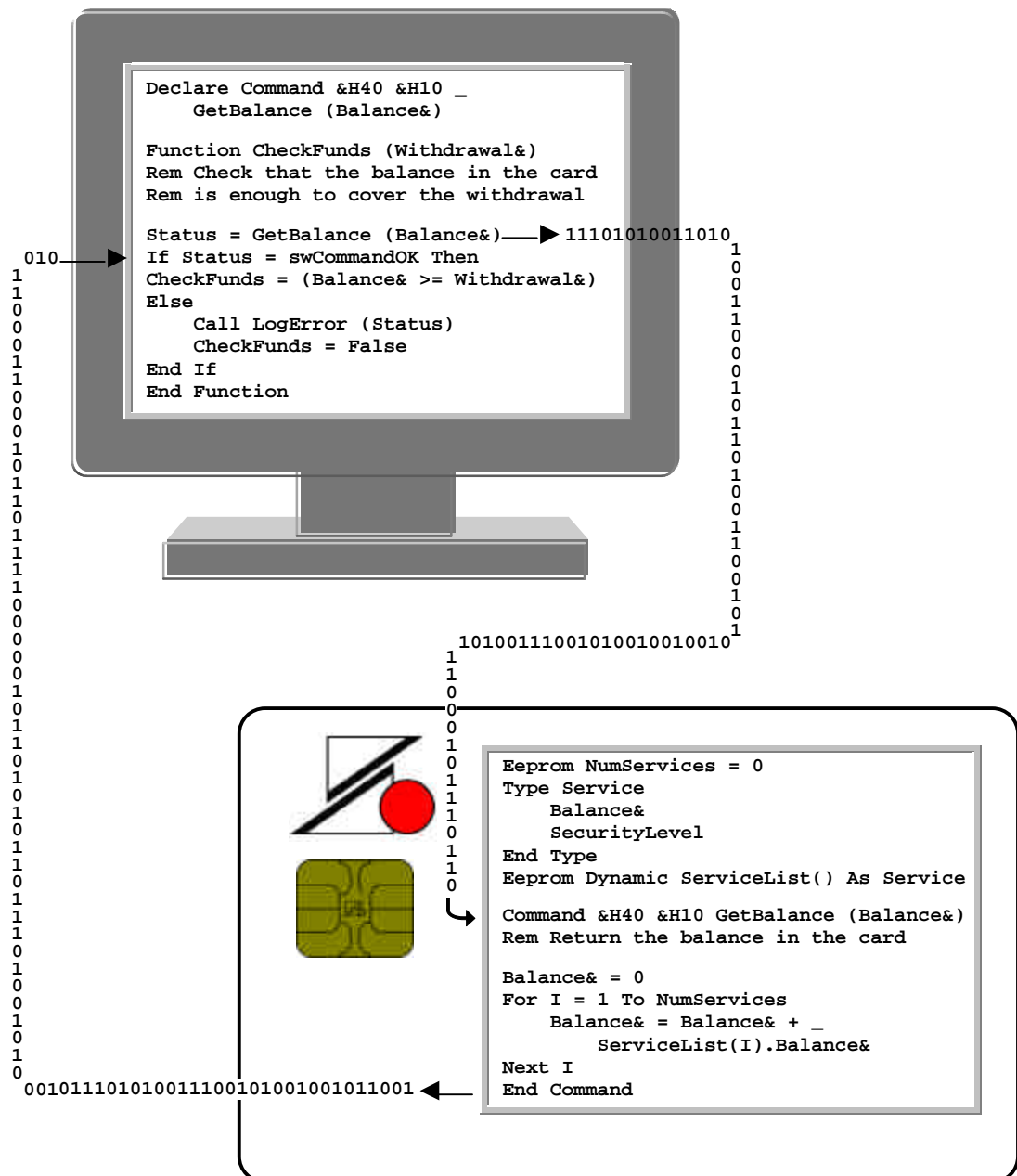


Professional BasicCard Datasheet



The ZeitControl Professional BasicCard Series

Document version 1.10
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>

Introduction

This document lists the features of all the currently available Professional BasicCard versions. Whenever a new Professional BasicCard is released, this document will be updated accordingly. The following cards are currently available:

ZC4.5A	RSA card with AES encryption
ZC4.5D	RSA card with DES encryption
ZC5.4	Elliptic Curve Cryptography with AES and DES encryption
ZC5.5	Elliptic Curve Cryptography with AES and DES encryption

This document gives the following information for each of these cards:

- the name of the card's configuration file
- the latest Operating System revision
- the size of available memory (**EEPROM** and **RAM**)
- cryptographic algorithms supported
- the default **ATR**
- library procedures available in the card
- compile-time options supported for the card

The ZC-Basic language, and the features common to all BasicCards, are described in the separate document **BasicCard: The Compact, Enhanced, and Professional BasicCards**, which can be downloaded from our website at <http://www.BasicCard.com>.

Series 4 Professional BasicCard

The Series 4 Professional BasicCard provides public-key cryptography based on the **RSA** algorithm. There are two versions: **ZC4.5A** (with symmetric encryption algorithm **AES**) and **ZC4.5D** (with symmetric encryption algorithm **DES**).

Professional BasicCard ZC4.5A

Configuration File

ZC45A_D.ZCF

Operating System Revision

ZC4.5A REV D

Available Memory

EEPROM	30816 (hex 7860) bytes
RAM	1024 (hex 400) bytes

Cryptographic Algorithms

RSA	Rivest-Shamir-Adleman public-key cryptography
AES	Advanced Encryption Standard (Rijndael) symmetric encryption algorithm
SHA-1	Secure Hash Algorithm, revision 1

Default ATR

3B FC 13 00 FF C0 80 31 80 75 ‘ZC4.5A REV C’ LRC
T=0 and T=1 protocols indicated.

Library Procedures

RSA Library

Function RsaPseudoPrime (*n\$, 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\$*)

AES Library

Function AES (*Type%, Key\$, Block\$*) **As String**
Only 128-bit keys are supported, i.e. *Type%* must be +/-128.

SHA Library

Function ShaHash (*S\$*) **As String**
Sub ShaStart (*HashBuff\$*)
Sub ShaAppend (*HashBuff\$, S\$*)
Function ShaEnd (*HashBuff\$*) **As String**

MISC Library

Sub RandomString (*S\$, Len%*)
Function LePresent()
Sub SuspendSW1SW2Processing()

Compile-Time Options

#Option T=0
#Option T=1
#Option T=0, T=1 (default)

Professional BasicCard ZC4.5D

Configuration File

ZC45D_D.ZCF

Operating System Revision

ZC4.5D REV D

Available Memory

EEPROM 30576 (hex **7770**) bytes
RAM 1024 (hex **400**) bytes

Cryptographic Algorithms

RSA Rivest-Shamir-Adleman public-key cryptography
DES Data Encryption Standard (Single/Triple) symmetric encryption algorithm
SHA-1 Secure Hash Algorithm, revision 1

Default ATR

3B FC 13 00 FF 40 80 ‘ZC4.5D REV D’
T=0 protocol indicated.

Library Procedures

RSA Library

Function RsaPseudoPrime (*n\$, 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\$*)

SHA Library

Function ShaHash (*S\$*) **As String**
Sub ShaStart (*HashBuff\$*)
Sub ShaAppend (*HashBuff\$, S\$*)
Function ShaEnd (*HashBuff\$*) **As String**

MISC Library

Sub RandomString (*S\$, Len%*)
Function LePresent()
Sub SuspendSW1SW2Processing()

Compile-Time Options

#Option T=0 (default)
#Option T=1
#Option T=0, T=1

Series 5 Professional BasicCard

The Series 5 Professional BasicCard provides public-key cryptography based on Elliptic Curves over the field $\text{GF}(2^{167})$. There are two versions, **ZC5.4** and **ZC5.5**, differing mainly in the amount of memory available. Both versions support symmetric encryption algorithms **AES** and **DES**.

Professional BasicCard ZC5.4

Configuration File

ZC54_C.ZCF

Operating System Revision

ZC5.4 REV C

Available Memory

EEPROM	16335 (hex 3FCF) bytes
RAM	686 (hex 2AE) bytes

Cryptographic Algorithms

EC-167	Elliptic Curve public-key cryptography over the field $\text{GF}(2^{167})$
AES	Advanced Encryption Standard (Rijndael) symmetric encryption algorithm
DES	Data Encryption Standard (Single/Triple) symmetric encryption algorithm
SHA-1	Secure Hash Algorithm, revision 1

Default ATR

3B FB 13 00 FF C0 80 31 80 75 ‘ZC5.4 REV C’ LRC
T=0 and T=1 protocols indicated.

Library Procedures

EC167 Library

Sub EC167SetPrivateKey (Key\$)
Function EC167SharedSecret (PublicKey\$) As String
Function EC167Sign (Hash\$) As String

AES Library

Function AES (Type%, Key\$, Block\$) As String
Only 128-bit keys are supported, i.e. Type% must be +/-128.

SHA Library

Function ShaHash (S\$) As String
Sub ShaStart (HashBuff\$)
Sub ShaAppend (HashBuff\$, S\$)
Function ShaEnd (HashBuff\$) As String

MISC Library

Sub RandomString (S\$, Len%)
Function LePresent()

Compile-Time Options

#Option T=0
#Option T=1
#Option T=0, T=1 (default)

#Option Allow9XXX
#Option InverseConvention

Professional BasicCard ZC5.5

Configuration File

ZC55_B.ZCF

Operating System Revision

ZC5.5 REV B

Available Memory

EEPROM	30975 (hex 78FF) bytes
RAM	1686 (hex 696) bytes

Cryptographic Algorithms

EC-167	Elliptic Curve public-key cryptography over the field GF (2 ¹⁶⁷)
AES	Advanced Encryption Standard (Rijndael) symmetric encryption algorithm
DES	Data Encryption Standard (Single/Triple) symmetric encryption algorithm
SHA-1	Secure Hash Algorithm, revision 1

Default ATR

3B FB 13 00 FF 81 31 80 75 ‘ZC5.5 REV B’ LRC
T=1 protocol indicated.

Library Procedures

EC167 Library

Sub EC167SetPrivateKey (Key\$)
Function EC167SharedSecret (PublicKey\$) As String
Function EC167Sign (Hash\$) As String
Function EC167Verify (Signature\$, Hash\$, PublicKey\$)

AES Library

Function AES (Type%, Key\$, Block\$) As String
All key lengths are supported: 128, 192, and 256 bits.

SHA Library

Function ShaHash (S\$) As String
Sub ShaStart (HashBuff\$)
Sub ShaAppend (HashBuff\$, S\$)
Function ShaEnd (HashBuff\$) As String

MISC Library

Sub RandomString (S\$, Len%)
Function LePresent()
Sub SuspendSW1SW2Processing()

Compile-Time Options

#Option T=0
#Option T=1 (default)
#Option T=0, T=1

#Option Allow9XXX