CONTENTS

1 DESCRIPTION .................................................. 3
2 BLOCK DIAGRAM ................................................ 4
3 FEATURES ......................................................... 5
   3.1 FAMILY STANDARD FEATURES ................................ 5
   3.2 SECURITY FEATURES ......................................... 5
   3.3 PRODUCT SPECIFIC FEATURES ................................. 5
   3.4 SUPPORT .................................................. 5
4 ORDERING INFORMATION ........................................ 6
5 PINNING INFORMATION .......................................... 6
   5.1 Bond pad assignments to Smart Card contacts and pin description ....................................... 6

Note: Specification may be changed without further notice.
1 DESCRIPTION

The P8WE5033 is a single chip secured 8-bit microcontroller, manufactured in a most advanced CMOS process. It is specifically designed for secured conditional access applications and transactions in smart card environments or other security applications.

As a member of the Philips Smart Card Controller family the P8WE5033 provides enhanced security features, which make the device suited for most high-end safeguarded applications, and is designed for embedding into chip cards according to ISO 7816.

To provide the highest possible degree of protection against hostile attacks the Philips Smart Card Controllers are designed for security which requires continuous ever ongoing improvements. Philips is committed to this policy. Special attention was drawn to the design of the security architecture, in order to achieve the high degree of protection against fraudulent attacks. Each security measure is designed to act as an integral part of the complete system in order to strengthen the design as a whole. The security measures are solely controlled by hardware and do not allow for software guided exceptions.

The P8WE5033 is a derivative of the 80C51 microcontroller family and has the same instruction set as the 80C51. The device includes 96 KBytes of ROM, 2304 bytes RAM (Data Memory) and 32 KBytes of EEPROM. The EEPROM features a data memory and a program memory usage mode. The non-volatile memory consists of high reliability memory cells to guarantee data integrity. This is especially important when the EEPROM is used as program memory.

The integrated co-processor FameX accelerates the encipherment for Public Key encryption algorithms. This widens the field of applications for this device, since it can be used as tamper-resistant security tool for secured and authentic communication in open networks.

The Triple-DES co-processor speeds up the calculation time for DES3 encryption by about three orders of magnitude compared to software solutions. Also single DES operations are supported.

Bi-directional communication with the device can be performed through three serial interface I/Os according to ISO standard 7816-3. The I/Os are under full control of the application software in order to allow for conditional controlled access to the different internal memories.

Further functionality is provided by two 16-bit timers and five vectorized interrupts from the I/Os, timers, EEPROM and FameX co-processor.

On-chip hardware is software controlled via Special Function Registers (SFRs). Their function and usage is described in the respective sections of the specification as the SFRs are correlated to the activities of the CPU, Interrupt, I/O, EEPROM, Timers, etc.

The P8WE5033 provides three power saving modes with reduced activity: the IDLE, the SLEEP and the CLOCK STOP mode. These three modes are activated by software.

The P8WE5033 operates with a single 3 V or 5 V power supply at a maximum clock frequency of 8 MHz. The set of more than 100 instructions is separated into 49 one-byte, 46 two-byte and 16 three-byte instructions.

With an input clock frequency of 8 MHz 64 instructions are executed in 0.75 µs and 45 instructions in 1.5 µs if default mode is selected. The double-clock mode offers the possibility to achieve the performance of a 10 MHz (internal) clock while supplying the device with a 5 MHz external clock (64 instructions are executed in 0.5 µs and 45 instructions in 1.0 µs).

The software development for the User ROM is supported by:

- Keil PK51 and DK51 development tool package incl. µVision2/dScope C51 simulator, additional specific CPU drivers and ISO 7816 card interface board (www.keil.com)
- Ashling Ultra-Emulator platform, stand alone ROM prototyping boards and ISO 7816 card interface board (www.ashling.com)
- Ashling Code Coverage and Performance Measurement software tools for real time software testing especially in the Smart Card terminal environment.
- Raisonance, RKitP51, RKitE51 Development Suite (includes RIDE, C-Compiler, Assembler, Simulator, card interface board and Realtime Emulator) (www.raisonance.com)

The P8WE5033 is available as sawn wafer and as semi-finished IC-card micro module. Prototyping is supported by a small-outline package (SO28).
2 BLOCK DIAGRAM

![Block diagram of P8WE5033 Smart Card Controller](image)

Fig.1 Block diagram P8WE5033.
3 FEATURES

3.1 FAMILY STANDARD FEATURES
• 8-bit 80C51 CPU
• Two 16-bit timers
• Multiple source vectorized interrupt system with two priority levels
• Multiple source reset system
• High reliable EEPROM for both, data storage and program execution
• Bytewise EEPROM programming and read access
• EEPROM endurance: minimum 100,000 programming cycles per byte
• EEPROM data retention time: 10 years minimum
• Power-saving IDLE mode
• Wake-up from IDLE mode by Reset or External Interrupt and also from internal interrupts of timers
• Low-power SLEEP and CLOCK STOP mode
• Wake-up from SLEEP and CLOCK STOP mode by Reset and External Interrupt
• Pad configuration according to ISO/IEC 7816: VSS, VDD, CLK, RST, I/O1
• Two additional I/Os, e.g. for full-duplex serial data communication; can be left unconnected if only one I/O is required.

3.2 SECURITY FEATURES
• Power-up / Power-down reset
• Low / high supply voltage sensor (LVS/HVS)
• Low / high clock frequency sensor (LFS/HFS)
• Low / high temperature sensor (LTS/HTS)
• On-chip self test with signature technique
• EEPROM programming:
  – no external clock
  – hardware sequencer controlled
  – on-chip high voltage generation
• Electronic fuses for safeguarded mode control
• 64 EEPROM bytes for customer-defined security FabKey. Featuring batch-, wafer- or die-individual security data.
• Clock Input Filter for protection against spikes
• Memory protection for RAM, EEPROM and ROM

3.3 PRODUCT SPECIFIC FEATURES
• 1 MHz to 8 MHz operating clock frequency range for program execution from both ROM or EEPROM
• Default mode: 6 clocks per instruction cycle
• Double clock mode: 3 clocks per instruction cycle
• Internal clock generation supported
• High speed Triple-DES co-processor
  – DES3 calculation time (including key load) < 200 µs
  – DES calculation time (including key load) < 100 µs
• Crypto Co-processor FameX (Fast Accelerator for Modular Exponentiation-eXtended) optimized for public key cryptographic calculations
  – the major Public Key Cryptosystems like RSA, El’Gamal, DSS, Diffie-Hellmann, Guillou-Quisquater, Fiat-Shamir and elliptic curve are supported
  – 4032 bits maximum key length for RSA with randomly chosen modulus
  – < 450 ms typical encryption time of 1024-bit RSA with randomly chosen modulus
  – 32-bit key length increments
  – boolean operations for acceleration of standard, symmetric cipher algorithms
• ISO UART supporting standard protocols T = 0 and T = 1 as well as high speed personalisation at 1 Mbits/s
• True random number generator in hardware
• 96 KBytes User ROM
• Memory Management System (MMS)
• Optional MOVC Blocking
• 32 KBytes EEPROM
• 32 bytes write-once area in EEPROM
• 256 bytes IDATA RAM
• 2048 bytes Extension RAM
• Versatile page mode EEPROM programming of 1 to 64 bytes at a time
• Typical EEPROM page mode programming time: 4.0 ms
• XRAM pointer for fast XRAM access.
• Warm Reset Indicator
• 2.7 V to 5.5 V extended operating voltage range
• –25 to +85 °C operating ambient temperature range
• 4 kV Electro Static Discharge (ESD) protection on ISO pads according to MIL Standard 883-C Method 3015.
• IDDQ testing for enhanced product reliability

3.4 SUPPORT
• Deliverable as sawn wafer on film frame carrier
• Deliverable as ISO7816 contact module
• Samples in small quantities in SO28 package
• Development support:
  – Keil 8051 simulator ‘PK51’, ‘DK51’
  – Ashling Microsystems development system with Windows based user interface.
  – Raisonance RKitP51, RKitE51 development suite
4 ORDERING INFORMATION

<table>
<thead>
<tr>
<th>TYPE NUMBER</th>
<th>PACKAGE DESCRIPTION</th>
<th>VERSION</th>
</tr>
</thead>
<tbody>
<tr>
<td>P8WE5033AEV/x..x</td>
<td>Module 8-contact Modules on super 35 mm film</td>
<td>SOT658AB2</td>
</tr>
<tr>
<td>P8WE5033AEW/x..x</td>
<td>FFC sawn wafer on film frame carrier</td>
<td>–</td>
</tr>
</tbody>
</table>

5 PINNING INFORMATION

5.1 Smart Card contacts

Fig. 2 ISO contact assignments for SOT658AB2.

Table 1 Pin description

<table>
<thead>
<tr>
<th>ISO 7816</th>
<th>P8WE5033</th>
</tr>
</thead>
<tbody>
<tr>
<td>CONTACTS</td>
<td>SYMBOL</td>
</tr>
<tr>
<td>C1</td>
<td>VCC</td>
</tr>
<tr>
<td>C2</td>
<td>RST</td>
</tr>
<tr>
<td>C3</td>
<td>CLK</td>
</tr>
<tr>
<td>C4</td>
<td>reserved</td>
</tr>
<tr>
<td>C5</td>
<td>GND</td>
</tr>
<tr>
<td>C6</td>
<td>VPP</td>
</tr>
<tr>
<td>C7</td>
<td>I/O</td>
</tr>
<tr>
<td>C8</td>
<td>reserved</td>
</tr>
</tbody>
</table>