

# SHORT FORM SPECIFICATION

**P8WE5017**

**Secure 8-bit Smart Card Controller**

Short Form Specification  
Revision 1.1

June 2001

---

**Secure 8-bit Smart Card Controller****P8WE5017**

---

**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	Smart Card contacts .....	6

**Note:** Specification may be changed without further notice.

# Secure 8-bit Smart Card Controller

# P8WE5017

## 1 DESCRIPTION

The P8WE5017 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 P8WE5017 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 P8WE5017 is a derivative of the 80C51 microcontroller family and has the same instruction set as the 80C51. The device includes 64 KBytes of ROM, 2304 bytes RAM (Data Memory) and 16 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 P8WE5017 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 P8WE5017 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  $\mu$ s and 45 instructions in 1.5  $\mu$ s 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  $\mu$ s and 45 instructions in 1.0  $\mu$ s).

The software development for the User ROM is supported by:

- Keil PK51 and DK51 development tool package incl.  $\mu$ Vision2/dScope C51 simulator, additional specific CPU drivers and ISO 7816 card interface board ([www.keil.com](http://www.keil.com))
- Ashling Ultra-Emulator platform, stand alone ROM prototyping boards and ISO 7816 card interface board ([www.ashling.com](http://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](http://www.raisonance.com))

The P8WE5017 is available as sawn wafer and as semi-finished IC-card micro module. Prototyping is supported by a small-outline package (SO28).

# Secure 8-bit Smart Card Controller

P8WE5017

## 2 BLOCK DIAGRAM

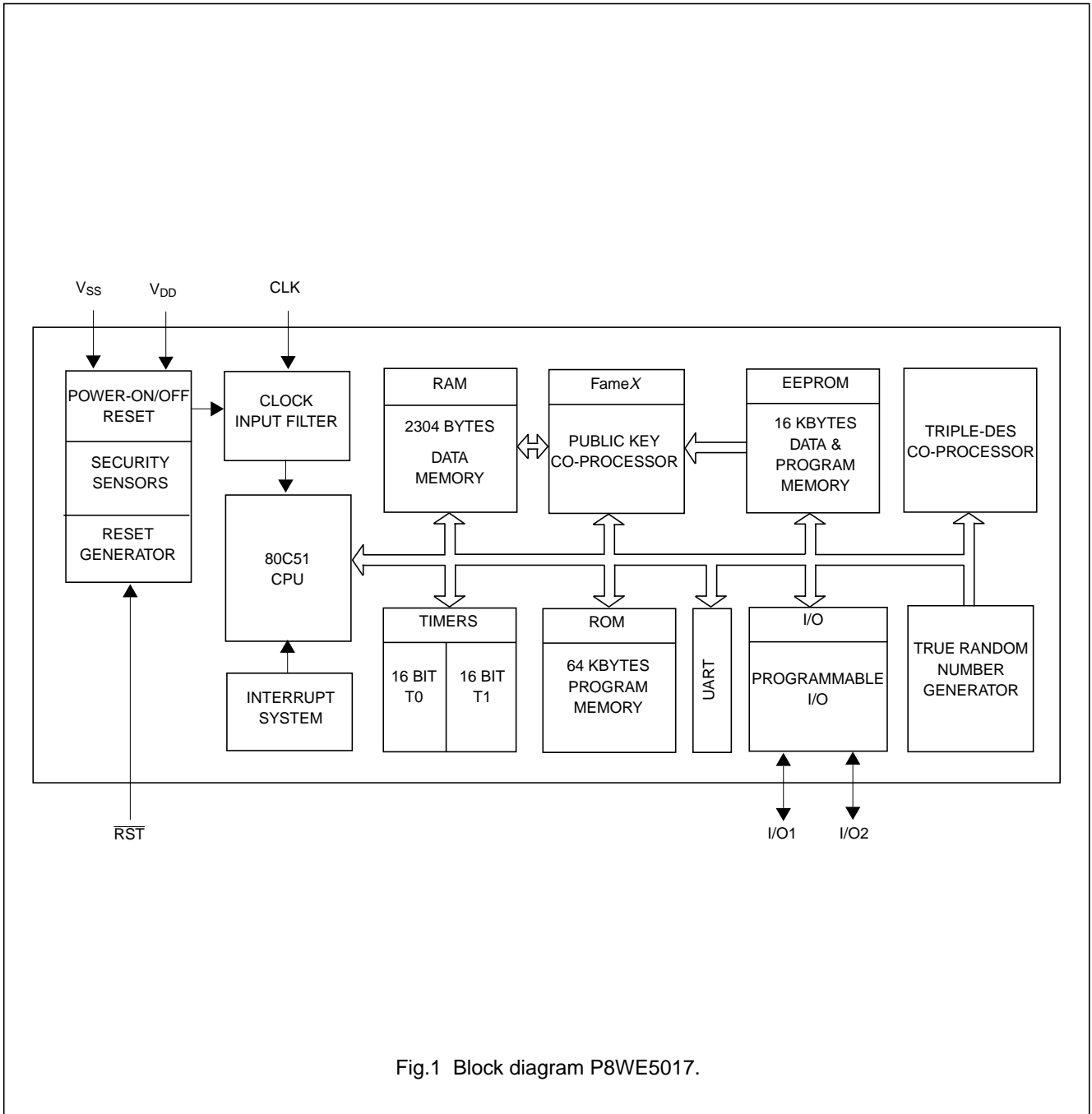


Fig.1 Block diagram P8WE5017.

# Secure 8-bit Smart Card Controller

# P8WE5017

## 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
- Byte-wise 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,  $\overline{RST}$ , I/O1
- Second 1-bit I/O port I/O2 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  $\mu$ s
  - DES calculation time (including key load) < 100  $\mu$ s
- 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
- 64 KBytes User ROM
- Memory Management System (MMS)
- Optional MOVN Blocking
- 16 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.
- I<sub>DDQ</sub> 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

## Secure 8-bit Smart Card Controller

P8WE5017

## 4 ORDERING INFORMATION

TYPE NUMBER	PACKAGE			TEMPERATURE RANGE (°C)
	NAME	DESCRIPTION	VERSION	
P8WE5017AEV/x..x	Module	8-contact Modules on super 35 mm film	SOT658AB2	-25 to +85
P8WE5017AEW/x..x	FFC	sawn wafer on film frame carrier	–	

## 5 PINNING INFORMATION

## 5.1 Smart Card contacts

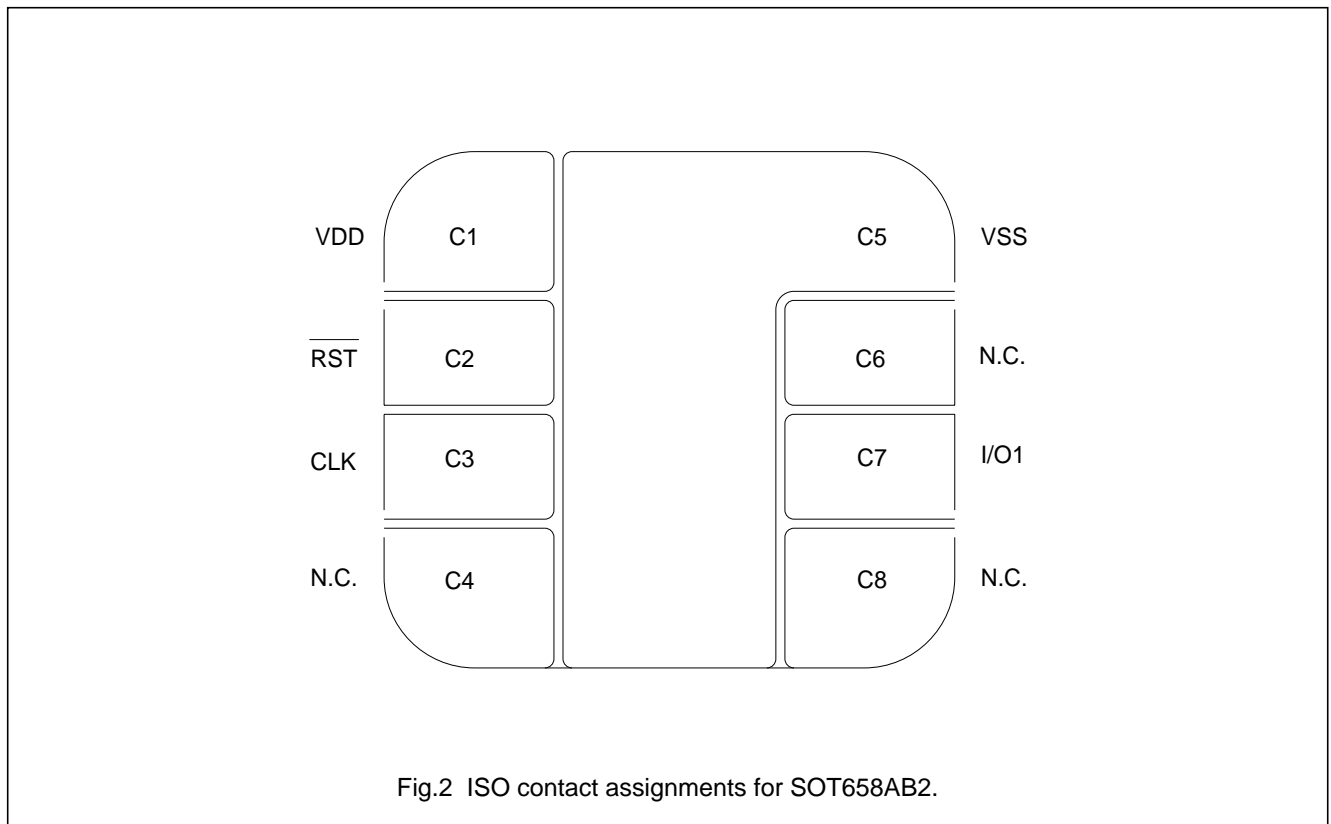


Table 1 Pin description

ISO 7816		P8WE5017	
CONTACTS	SYMBOL	SYMBOL	DESCRIPTION
C1	VCC	VDD	Power supply voltage input
C2	RST	$\overline{\text{RST}}$	Reset input, active LOW
C3	CLK	CLK	Clock input
C4	reserved	N.C.	not connected
C5	GND	VSS	Ground (reference voltage) input
C6	VPP	N.C.	not connected
C7	I/O	I/O1	Input/Output #1 for serial data
C8	reserved	N.C.	not connected

# Philips Semiconductors – a worldwide company

**Argentina:** see South America

**Australia:** 34 Waterloo Road, NORTH RYDE, NSW 2113, Tel. +61 2 9805 4455, Fax. +61 2 9805 4466

**Austria:** Computerstr. 6, A-1101 WIEN, P.O. Box 213, Tel. +43 160 1010, Fax. +43 160 101 1210

**Belarus:** Hotel Minsk Business Center, Bld. 3, r. 1211, Volodarski Str. 6, 220050 MINSK, Tel. +375 172 200 733, Fax. +375 172 200 773

**Belgium:** see The Netherlands

**Brazil:** see South America

**Bulgaria:** Philips Bulgaria Ltd., Energoproject, 15th floor, 51 James Bourchier Blvd., 1407 SOFIA, Tel. +359 2 689 211, Fax. +359 2 689 102

**Canada:** PHILIPS SEMICONDUCTORS/COMPONENTS, Tel. +1 800 234 7381

**China/Hong Kong:** 501 Hong Kong Industrial Technology Centre, 72 Tat Chee Avenue, Kowloon Tong, HONG KONG, Tel. +852 2319 7888, Fax. +852 2319 7700

**Colombia:** see South America

**Czech Republic:** see Austria

**Denmark:** Prags Boulevard 80, PB 1919, DK-2300 COPENHAGEN S, Tel. +45 32 88 2636, Fax. +45 31 57 0044

**Finland:** Sinikalliontie 3, FIN-02630 ESPOO, Tel. +358 9 615800, Fax. +358 9 61580920

**France:** 4 Rue du Port-aux-Vins, BP317, 92156 SURESNES Cedex, Tel. +33 1 40 99 6161, Fax. +33 1 40 99 6427

**Germany:** Hammerbrookstraße 69, D-20097 HAMBURG, Tel. +49 40 23 53 60, Fax. +49 40 23 536 300

**Greece:** No. 15, 25th March Street, GR 17778 TAVROS/ATHENS, Tel. +30 1 4894 339/239, Fax. +30 1 4814 240

**Hungary:** see Austria

**India:** Philips INDIA Ltd, Band Box Building, 2nd floor, 254-D, Dr. Annie Besant Road, Worli, MUMBAI 400 025, Tel. +91 22 493 8541, Fax. +91 22 493 0966

**Indonesia:** see Singapore

**Ireland:** Newstead, Clonskeagh, DUBLIN 14, Tel. +353 1 7640 000, Fax. +353 1 7640 200

**Israel:** RAPAC Electronics, 7 Kehilat Saloniki St, PO Box 18053, TEL AVIV 61180, Tel. +972 3 645 0444, Fax. +972 3 649 1007

**Italy:** PHILIPS SEMICONDUCTORS, Piazza IV Novembre 3, 20124 MILANO, Tel. +39 2 6752 2531, Fax. +39 2 6752 2557

**Japan:** Philips Bldg 13-37, Kohnan 2-chome, Minato-ku, TOKYO 108, Tel. +81 3 3740 5130, Fax. +81 3 3740 5077

**Korea:** Philips House, 260-199 Itaewon-dong, Yongsan-ku, SEOUL, Tel. +82 2 709 1412, Fax. +82 2 709 1415

**Malaysia:** No. 76 Jalan Universiti, 46200 PETALING JAYA, SELANGOR, Tel. +60 3 750 5214, Fax. +60 3 757 4880

**Mexico:** 5900 Gateway East, Suite 200, EL PASO, TEXAS 79905, Tel. +9-5 800 234 7381

**Middle East:** see Italy

**Netherlands:** Postbus 90050, 5600 PB EINDHOVEN, Bldg. VB, Tel. +31 40 27 82785, Fax. +31 40 27 88399

**New Zealand:** 2 Wagener Place, C.P.O. Box 1041, AUCKLAND, Tel. +64 9 849 4160, Fax. +64 9 849 7811

**Norway:** Box 1, Manglerud 0612, OSLO, Tel. +47 22 74 8000, Fax. +47 22 74 8341

**Philippines:** Philips Semiconductors Philippines Inc., 106 Valero St. Salcedo Village, P.O. Box 2108 MCC, MAKATI, Metro MANILA, Tel. +63 2 816 6380, Fax. +63 2 817 3474

**Poland:** Ul. Lukiska 10, PL 04-123 WARSZAWA, Tel. +48 22 612 2831, Fax. +48 22 612 2327

**Portugal:** see Spain

**Romania:** see Italy

**Russia:** Philips Russia, Ul. Usatcheva 35A, 119048 MOSCOW, Tel. +7 095 755 6918, Fax. +7 095 755 6919

**Singapore:** Lorong 1, Toa Payoh, SINGAPORE 1231, Tel. +65 350 2538, Fax. +65 251 6500

**Slovakia:** see Austria

**Slovenia:** see Italy

**South Africa:** S.A. PHILIPS Pty Ltd., 195-215 Main Road Martindale, 2092 JOHANNESBURG, P.O. Box 7430 Johannesburg 2000, Tel. +27 11 470 5911, Fax. +27 11 470 5494

**South America:** Rua do Rocio 220, 5th floor, Suite 51, 04552-903 São Paulo, SÃO PAULO - SP, Brazil, Tel. +55 11 821 2333, Fax. +55 11 829 1849

**Spain:** Balmes 22, 08007 BARCELONA, Tel. +34 3 301 6312, Fax. +34 3 301 4107

**Sweden:** Kottbygatan 7, Akalla, S-16485 STOCKHOLM, Tel. +46 8 632 2000, Fax. +46 8 632 2745

**Switzerland:** Allmendstrasse 140, CH-8027 ZÜRICH, Tel. +41 1 488 2686, Fax. +41 1 481 7730

**Taiwan:** Philips Semiconductors, 6F, No. 96, Chien Kuo N. Rd., Sec. 1, TAIPEI, Taiwan Tel. +886 2 2134 2865, Fax. +886 2 2134 2874

**Thailand:** PHILIPS ELECTRONICS (THAILAND) Ltd., 209/2 Sanpavuth-Bangna Road Prakanong, BANGKOK 10260, Tel. +66 2 745 4090, Fax. +66 2 398 0793

**Turkey:** Talatpasa Cad. No. 5, 80640 GÜLTEPE/ISTANBUL, Tel. +90 212 279 2770, Fax. +90 212 282 6707

**Ukraine:** PHILIPS UKRAINE, 4 Patrice Lumumba str., Building B, Floor 7, 252042 KIEV, Tel. +380 44 264 2776, Fax. +380 44 268 0461

**United Kingdom:** Philips Semiconductors Ltd., 276 Bath Road, Hayes, MIDDLESEX UB3 5BX, Tel. +44 181 730 5000, Fax. +44 181 754 8421

**United States:** 811 East Arques Avenue, SUNNYVALE, CA 94088-3409, Tel. +1 800 234 7381

**Uruguay:** see South America

**Vietnam:** see Singapore

**Yugoslavia:** PHILIPS, Trg N. Pasica 5/v, 11000 BEOGRAD, Tel. +381 11 625 344, Fax. +381 11 635 777

**For all other countries apply to:** Philips Semiconductors, Marketing & Sales Communications, Building BE-p, P.O. Box 218, 5600 MD EINDHOVEN, The Netherlands, Fax. +31 40 27 24825

**Internet:** <http://www.semiconductors.philips.com>

© Philips Electronics N.V. 1997

SCA55

All rights are reserved. Reproduction in whole or in part is prohibited without the prior written consent of the copyright owner.

The information presented in this document does not form part of any quotation or contract, is believed to be accurate and reliable and may be changed without notice. No liability will be accepted by the publisher for any consequence of its use. Publication thereof does not convey nor imply any license under patent- or other industrial or intellectual property rights.

*Let's make things better.*

**Philips  
Semiconductors**



**PHILIPS**