SHORT FORM SPECIFICATION

P16WX064

Smart*XA*-Family

Secure 16-bit Smart Card Controller

Short Form Specification February 2001
Revision 1.1

Philips
Semiconductors

PHILIPS

CONTENTS

Note: Specification may be changed without further notice.

Smart*XA*-Family
Secure 16-bit Smart Card Controller

P16WX064

1 DESCRIPTION

Philips Semiconductors Smart*XA* (eXtended Architecture) is a secure 16-bit microcontroller, manufactured in an advanced CMOS process. It is a major part of Philips Smart Card Controller ICs family concept offering a complete product range suiting the different needs of up coming Smart Card generations.

The Smart*XA* 2nd generation with extended memory and enhanced security features fulfils the increasing requirements of secure multi-application in a multi-provider environment. It is designed for embedding into chip cards according to ISO 7816.

The high performance of its true 16-bit CPU easily handles the requirements of high performance, high security applications. Furthermore it provides an optimum support for interpreter based languages taking into account the low power demand of e.g. mobile communication application. The Smart*XA* 2nd generation is an ideal base for future open software platform concepts.

Special attention was drawn to the design of the security architecture, in order to achieve the high degree of protection against attacks. Each security measure is designed to act as an integral part of the complete security 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 Smart*XA* 2nd generation is the right choice for users looking for high performance and secure multi application. Its unique hardware firewall concept, build on three operation modes and an extended memory management unit provides the integrity of multiple application and its data and also allows secure download of applications.

The EEPROM memory can be used as data memory or as program memory. It contains a high reliability cell which guarantees data integrity. This is especially important when the EEPROM is used as memory for native programs.

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

A Triple-DES co-processor together with a True Random Number Generator (TRNG) and a Cyclic Redundancy Code (CRC) unit complete the leading edge technology and security of the product family.

The bi-directional communication with the device can be performed through two serial interface I/Os according to ISO standard 7816-3. The I/Os can run under full control of the kernel operating system (System mode) software in order to allow for conditional controlled access to the different internal memories.

Further functionality is provided by a UART equipped with a DMA for Direct Memory Access for fast serial data transfer according ISO/IEC 7816-3 to accomplish fast personalization time. Additional there are two 16-bit timers, which can be used as baud rate generator or time-out of serial data transmission and task timing control, seven vectorized interrupts from the I/Os, timers, UART, EEPROM, Fame*X* co-processor and Triple-DES co-processor.

Philips Semiconductors P16WX064 is the first product of its smart card controller family equipped with an USB interface according to USB version 1.1. It allows flexible interfacing, e.g. easy PC-access without the need for a smart card reader.

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

The P16WX064 operates with a single 3 V or 5 V power supply at a maximum clock frequency of 6 MHz.

The software development for the User ROM is supported by

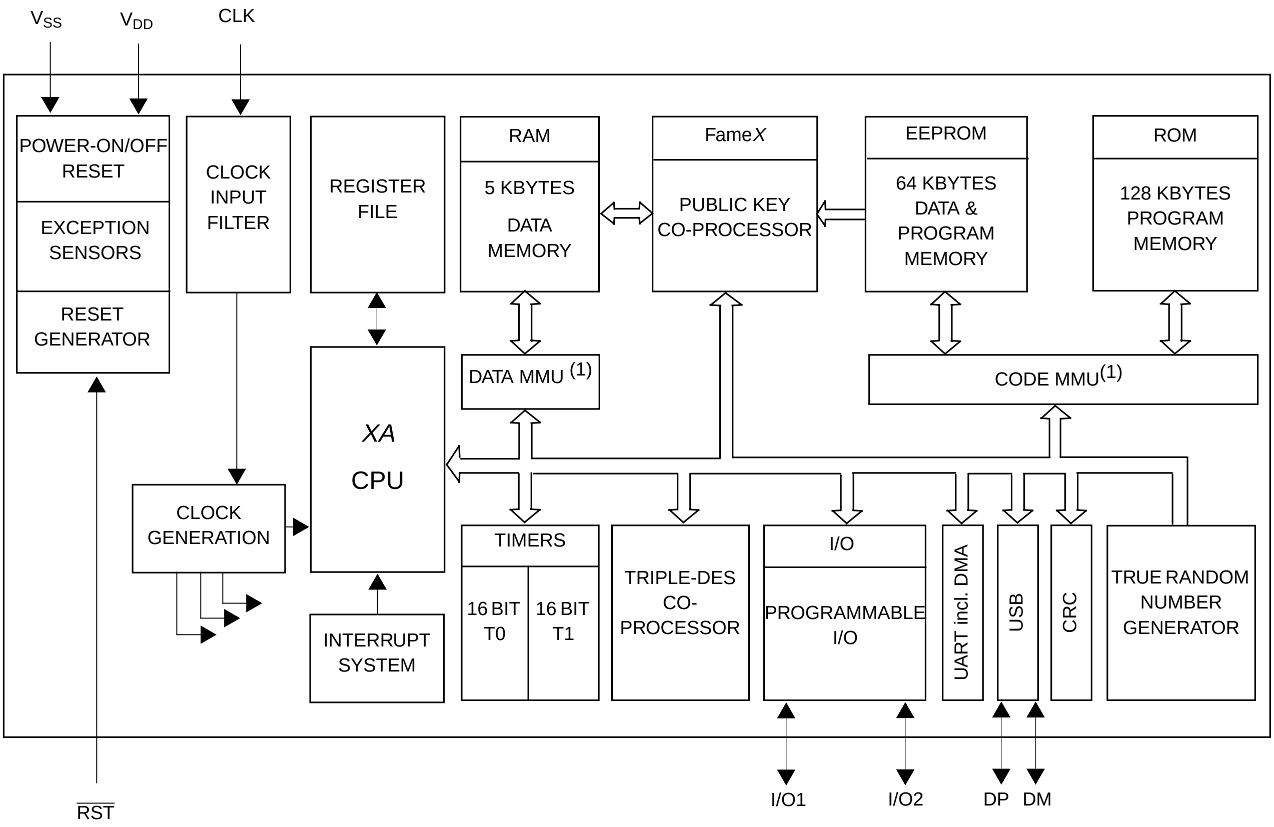
- Ashling Ultra-Emulator platform, stand alone ROM prototyping boards and ISO 7816 card interface board *(www.ashling.com)*
- Raisonance, RKitPXA, RKitEXA Development Suite (includes RIDE, C-Compiler, Assembler, Simulator, card interface board and Realtime Emulator) *(www.raisonance.com)*
- Tasking C-Compiler *(www.tasking.com)*

for real-time testing of the firmware especially in the Smart Card terminal environment.

On-chip hardware functions are controlled via Special Function Registers (SFRs). Their usage is described in the respective sections of this specification as the SFRs are correlated to the activities of CPU, Memory Management Unit, EEPROM, Interrupt, I/O, Timer 0/1, etc.

The P16WX064 is available as sawn wafer. Prototyping is supported by a small-outline package (SO28).

2 BLOCK DIAGRAM



(1) MMU = Memory Management Unit

Fig.1 Block Diagram P16WX064.

3 FEATURES

3.1 FAMILY STANDARD FEATURES

- Full 16-bit architecture
  - 16-bit fully static CPU
  - Harvard architecture: separate data- and program memory
  - user configurable support for an unified memory model
  - EEPROM for data storage and program execution
- Hardware firewall security providing System mode, Meta mode and User mode with memory protection
- Dynamic Memory Management Unit (MMU) for program and data memory
- 4 Mbytes program memory address range with ROM and EEPROM
- 1 MByte data memory address range with RAM and EEPROM
- Versatile page mode EEPROM programming
- Byte/Wordwise EEPROM read access
- True Random Number Generator
- UART for fast serial data transfer
  - according ISO/IEC 7816-3, supporting protocol types T=0 and T=1
  - to accomplish fast personalization
  - to provide fast application download capabilities
  - DMA access to RAM for transmission and reception without CPU involvement
- 21 16-bit CPU registers
  - 4 banks of R0 to R3 registers for fast context switching plus R4 to R7 registers, each capable of performing all arithmetic and logic operations
  - separate stack pointers for System mode and User mode
- Complex instruction set
  - all commands scalable as 8 or 16-bit
  - tailored for high level languages
  - including bit-wise operations as well as fast 16 x 16 multiply and 32/16 divide
- Multi-tasking and real-time executive support with
  - flexible interrupt structure
  - segmented data memory
  - multiple stacks for easy context-switching
- Multiple source vectorized interrupt system comprising
  - 16 software trap interrupts
  - 7 hardware event interrupts
  - 7 software interrupts
  - 7 system exception interrupts
- Multiple source reset system
- Power-saving IDLE mode
- Low-power SLEEP and CLOCK STOP mode
- I/O-interface for S/W, and H/W functions UART and External Interrupt
- Pad configuration according to ISO 7816-3: VSS, VDD, CLK, $\overline{\text{RST}}$, I/O1
- Second 1-bit I/O port for full-duplex serial data communication; can be left unconnected if only one I/O is required.

3.2 SECURITY FEATURES

- Hardware firewall and dynamic MMU
- Power-on reset
- Low supply voltage sensor (LVS)
- High supply voltage sensor (HVS)
- Low clock frequency sensor (LFS)
- High clock frequency sensor (HFS)
- High temperature sensor (HTS)
- Low temperature sensor (LTS)
- Clock input filter for protection against spikes
- On-chip self test utilizing signature techniques
- EEPROM programming timing independent from external clock
- EEPROM programming operation controlled by hardware sequencer
- On-chip EEPROM programming voltage generation
- Electronic fuses for safeguarded mode and write access control
- 64 EEPROM bytes for customer-defined security FabKey, featuring batch-, wafer- or die-individual security data
- 64 EEPROM bytes OTP (One-Time-Programmable) security data, featuring 512 program-only flags which can be used in System mode as irreversible event memory.

3.3 SUPPORT

- Deliverable as wafer, sawn wafer on film frame carrier or as modules
- ISO 7816 contact module
- Samples in small quantities in SO28 package
- Development support:
  - – Ashling Microsystems development system with Windows based user interface
  - – Raisonance RKitPXA, RKitEXA development suite
- Preservation of customer investments ensured by
  - – Instruction set identical with Philips 80C51 XA [same (C) compiler, (macro) assembler and libraries (of tools or self-developed)]
  - – Smooth design transitions for upgrades

3.4 P16WX064 PRODUCT SPECIFIC FEATURES

- 128 KBytes User ROM
- 4 K + 1056 bytes DATA RAM
- 64 KBytes EEPROM
- Versatile page mode EEPROM programming of 1 to 128 bytes at a time
- Typical EEPROM page mode programming time:
  4.0 ms (with normal Program mode)
  2.0 ms (with Program Only mode) [1]
- 32 ms/1 KByte, i.e. 2s for full 64 KBytes EEPROM (normal program mode)

  16 ms/1 KByte, i.e. 1s for full 64 KBytes EEPROM (program only mode)
- EEPROM endurance: minimum 100.000 programming cycles per byte
- EEPROM data retention time: 10 years minimum
- Crypto co-processor Fame*X* (Fast Accelerator for Modular Exponentiation-e*X*tended) 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 cryptosystems (ECC) are supported
  - – 2048 bits maximum key length for RSA with randomly chosen modulus
  - – 3 register banks for fast operation mode switching
  - – < 400 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
- High speed Triple-DES co-processor
  - – DES3 calculation time (including key load) < 110 µs
- CRC-16, CRC-32 Module.
  - – supporting three different polynomials
  - – real-time CRC calculation without adding wait states
  - – three different sources selectable for CRC calculation:
    - - Data Memory read & write
    - - Code Memory read & write
    - - Instruction codes from currently executed opcode
- Two 16-bit Timers/Counters
  - – individually configurable
  - – internal CPU clock is the basic clock in timer modes
  - – ISO UART's bit-time (etu) events are sensed in the counter mode
- ISO UART supporting standard ISO/IEC 7816-3 protocols T=0 and T=1 as well as high speed enhancement (personalisation up to $^{3}/_{4}$ Mbit/s)
- UART DMA
  - – CPU independent transmission of data from UART to data memory and vice versa
  - – full configurable in the addressable RAM range
- Universal Serial Bus Interface
  - – compliant to USB specification Rev 1.1
  - – 1.5 Mbit/s USB low-speed function
  - – USB bus-powered capability
  - – SoftConnect™: software controllable bus connect option
  - – two clock options: external 6 MHz CLK or internally generated clock
- Software configurable Clock System
  - – CPU clock
    - External CLK: 1 to 6 MHz
    - Internal clock: 1, 4, 8, or 16 MHz
  - – Triple-DES clock is always 2 times the CPU clock
  - – Fame*X* clock
    is configured independent from the CPU clock
    - External CLK: 1 to 6 MHz
    - Internal clock: 8, 16, or 32 MHz

[1] requires EEPROM delivery state Full Erase

- Timers/Counters
  - Basic TIMER clock is always the CPU clock. Timer mode increment rate is configurable via prescalers, individually for Timer 0 and Timer 1, for basic clock frequency division by
    - ∗ 1
    - ∗ 4
    - ∗ 16
    - ∗ 64
  - COUNTER mode
    provides counting of ISO UART etu events
- ISO UART Baudrate
  Basic ISO UART clock is always the external CLK: 1 to 6 MHz. UART 'bit rate adjustment' and 'clock rate conversion' configurable via
  - Baudrate timer overflow rate
  - UART prescaler for overflow rate division by
    - ∗ 4 (proprietary high-speed mode):
      up to 750.0 kbit/s @ f_{CLK} = 6.0000 MHz
    - ∗ 31 (ISO/IEC 7816-3):
      9.6 to 115.2 kbit/s @ f_{CLK} = 3.5712 MHz
    - ∗ 32 (ISO/IEC 7816-3):
      9.6 to 153.6 kbit/s @ f_{CLK} = 4.9152 MHz

- Wake-up from SLEEP and CLOCK STOP mode by Reset, External or USB Interrupt
- Wake-up from IDLE mode by Reset, External Interrupt, Timer, UART or USB Interrupts
- 2.7 V to 5.5 V operating voltage range for ISO chip card contact UART operation
- 4.0 V to 5.5 V operating voltage range for USB operation
- –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
- Controlled I_{DDQ} test for enhanced product reliability.

4 ORDERING INFORMATION

TYPE NUMBER	PACKAGE			TEMPERATURE RANGE (°C)
	NAME	DESCRIPTION	VERSION	
P16WX064AEW/x..x	FFC	sawn wafer on film frame carrier	–	–25 to +85

5 PINNING INFORMATION

5.1 Smart Card contacts

In an application a hybrid USB/ISO Smart Card is used either as a USB interface device, as an ISO/IEC 7816-3 T=0 or T=1 integrated circuit card, or as a device that utilizes the P16WX064 proprietary extensions to the ISO-UART. Applications are not using the Universal Serial Bus interface and the ISO-UART at the same time.

Three different Chip Card contact assignments may be chosen. The characteristical differences are:

1. Standard ISO 7816 UART contact interface (see Fig.2)

   - IC pin I/O1 is bonded to card contact C7 (I/O)

   - C4 and C8 are not bonded

2. ISO 7816 UART contact interface plus proprietary 2nd I/O (see Fig.3)

   - IC pin I/O1 is bonded to card contact C7 (I/O or I/O1)

   - IC pin I/O2 is bonded to card contact C8 (I/O2)

   - C4 is not bonded

3. Hybrid USB/ISO 7816 UART contact interface (see Fig.4)

   - IC pin I/O1 is bonded to card contact C7 (I/O)

   - IC pin DP is bonded to card contact C8 (D+)

   - IC pin DM is bonded to card contact C4 (D-)

- USB power line VBUS is to be connected to card contact C1 (VDD) in bus-powered applications.
- USB ground line GND is to be connected to card contact C5 (VSS).
- USB data line D- is to be connected to card contact C4 (DM).
- USB data line D+ is to be connected to card contact C8 (DP).
- C2 (RST) must be connected to VBUS.
- C3 (CLK) can be sourced from an external 6.00 MHz clock signal, or may be connected with GND, or may be left unconnected.
- C6 (N.C.) is internally not connected to the IC.
  C6 should be left unconnected, or be connected to C5 (VSS) or to C1 (VDD).
- C7 (I/O1) can be left unconnected, or it can be used for external I/O functions. I/O1 is accessible by system software as a Special Function Register bit, and it can be used as external interrupt request input.
- IC port I/O2 is not externally available in 8-contact chip card modules with USB bonding. In packages like Hybrid USB/ISO Smart Card Contact Assignments.

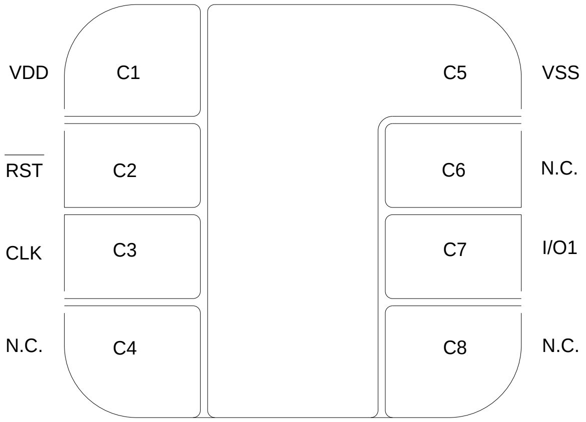


Fig.2 Standard Chip Card Contact Configuration according to ISO 7816.

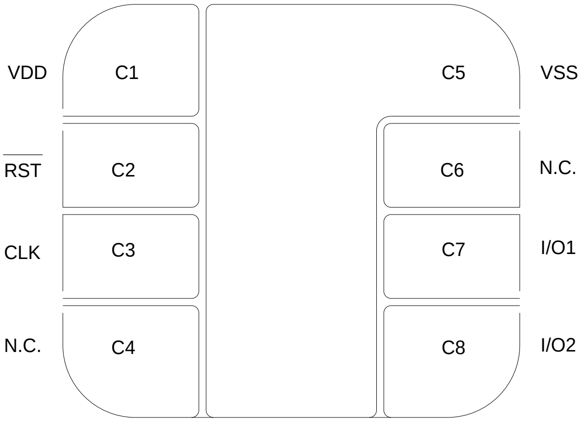


Fig.3 Chip Card Contact Configuration ISO7816 + 2nd I/O[1].

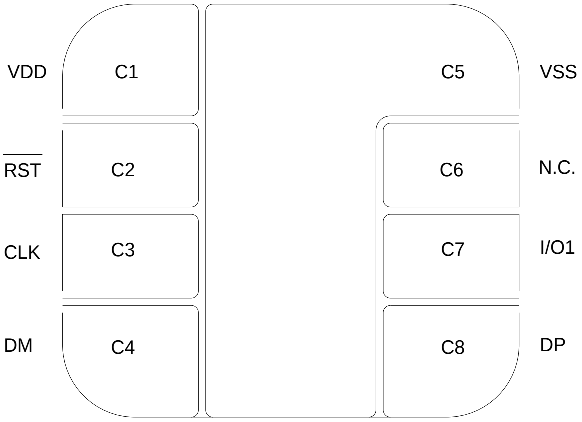


Fig.4 Hybrid USB/ISO 7816 UART Chip Card Contact Configuration.

[1] *This is the standard wiring for the Philips Chip Card Module.*

Table 1 Bond pad assignments to Smart Card contacts according to ISO 7816-2

ISO 7816		USB/ISO7816 HYBRID	P16WX064
CONTACTS	**SYMBOL**	**SYMBOL**	**DESCRIPTION**
C1	VCC	VDD	Power supply voltage input
C2	RST	RST	Reset input, active LOW
C3	CLK	CLK	Clock input
C4	reserved		not connected, or
C4		DM	USB I/O D- connection
C5	GND	VSS	Ground (reference voltage) input
C6	VPP	N.C.	not connected
C7	I/O	I/O1	ISO7816 Input/Output #1 for serial data
C8	reserved		not connected, or
C8			Input/Output #2 for serial data, or
C8		DP	USB I/O D+ connection

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

SCA55

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