

# SHORT FORM SPECIFICATION

**SmartMX**

**P5CC018**

Secure Smart Card Controller

Objective Specification  
Revision 1.0

2003 April 08

## Secure Smart Card Controller

P5CC018

## CONTENTS

1	DESCRIPTION .....	3
1.1	The SmartMX Architecture .....	3
1.2	The SmartMX Contact Interface .....	3
1.3	The FameXE .....	4
1.4	The Hardware Triple DES (Digital Encryption Standard) Accelerator .....	4
1.5	The Hardware AES (Advanced Encryption Standard) Accelerator .....	4
1.6	Security Features .....	4
1.7	PRODUCT TYPES .....	5
1.8	P5CC018 device .....	5
2	BLOCK DIAGRAM .....	6
3	FEATURES .....	7
3.1	Family Standard Features .....	7
3.2	Security Features .....	8
3.3	Product Specific Features .....	8
3.4	Design-in Support .....	9
4	ORDERING INFORMATION .....	10
5	PINNING INFORMATION .....	11
5.1	Smart Card contacts .....	11
5.1.1	Smart Card contacts "Standard Type" .....	11

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

---

## Secure Smart Card Controller

## P5CC018

---

### 1 DESCRIPTION

Philips Semiconductor's SmartMX (Memory eXtension) is a fully compatible and significantly enhanced 80C51 architecture, called MX51 architecture. The SmartMX family forms a combined WE-family and RF-family MIFARE® ProX) successor platform, positioned to service high volume, cost sensitive, mono- and multi-application markets including banking/finance, mobile communications, conditional access, pay TV, government, network access and transportation. SmartMX enables the easy implementation of state-of-the-art operating systems and open platform solutions including Java Card Open Platform and MULTOS and offers an optimized feature set together with the highest levels of security. Within its targeted segment, the new platform is the most advanced solution available, combining exceptionally powerful co-processors for public and secret key encryption to support RSA, ECC, DES and AES, with the high security, low power, performance optimized design concept of Philips Semiconductors' TANGRAM technology. SmartMX is manufactured using most advanced CMOS 0.18  $\mu$  structures, featuring 5 metal layer technology and supports Class "A", "B" and "C" voltage ranges (1.62 - 5.5V) as required by application standards such as 3rd Generation Mobile Communication (3GPP) and the credit/debit card standard (EMV).

With extended support for cryptography and multiple interface options, SmartMX is the optimal choice for use in almost any IT environment. It is the first solution of its kind to incorporate three interface options as an integral part of a highly secure smart card controller platform – ISO 7816 Contact Interface, ISO 14443A Contactless Interface and USB 1.1 Interface. Within indicated family members it features a state-of-the-art Memory Management Unit (MMU) to enhance the security of the platform in a multi-application set up. All products include additional features for significantly improved execution speed, enhanced functionality and expanded on-chip memory configurations of more than 500 Kbytes this making it the most powerful smart card IC-platform of its kind. All functions featured, including the operation of FameXE, DES and AES, are available and fully operational on the contactless interface.

#### 1.1 The SmartMX Architecture

SmartMX is based on Philips Semiconductors' 8051 architecture-based MX-concept and offers an absolute linear addressing range for all on-chip memory up to 8 Mbytes meaning programmers do not have to worry about addressing limitations and related paging concepts. A new set of instructions has been added to the 8051 instruction set to support the extended addressing concept and improve the code efficiency with C programming. MX development tools generate a software code that is up to 30% more condensed than for std 8051 architectures, and which enable higher performance at minimized memory space consumption. MX maintains 100% backward compatibility to Philips Semiconductors' well established WE family and enables an easy transition of existing software retaining available software assets of Philips WE-Family and MIFARE® ProX-family customers and other 8051-based software developments. A "WE-compatibility mode" provides for direct reuse of existing WE software within SmartMX family. Together with Philips advanced 0.18  $\mu$ m technology and the high performing, power saving, TANGRAM design methodology, SmartMX will operate at clock frequencies of up to 30 MHz, outperforming any other comparable platform.

#### 1.2 The SmartMX Contact Interface

Operating in accordance with ISO 7816, the SmartMX contact interface is supported by a built in UART, which enables data rates of up to 1M-bit/s allowing for the automatic generation of all typical baud rates.

---

## Secure Smart Card Controller

## P5CC018

---

### 1.3 The FameXE

Philips Semiconductors' solution to support public key cryptography based on finite fields of prime order – GF(p), has been enhanced from FameX to become FameXE within the SmartMX family concept. FameXE supports the trend of increasing RSA keys with faster execution speeds and Elliptic Curve Cryptography (ECC) based on GF(2n) at best performance. FameXE supports RSA with an operand length of up to 5kBits and related standards (PKC#1[RSA], PKC#3 [Diffie-Hellman] and FIPS 186-2 [DSA&EC-DSA], IEEE P1363).

The FameXE co-processor also supports ECC key lengths of up to 192-bit, which according to the German BSI is comparable with 2048-bit RSA [1]. An ECC – GF(2n) based signature, using a 163-bit key can be executed in less than 30ms providing a security level comparable to 1024-bit RSA. FameXE is easy to use and understood by programmers. Its user friendly and flexible interface provides programmers with the freedom to implement their own know how without being obliged to use third party software. A cryptolibrary providing a large range of required functions is available to support customers in implementing Public Key-based solutions.

### 1.4 The Hardware Triple DES (Digital Encryption Standard) Accelerator

The Digital Encryption Standard (DES) for symmetric encryption is still used in most applications today and is supported by a dedicated, high performance, highly attack resistant co-processor. Single DES and triple DES, based on two or three DES keys, can be executed within less than 50  $\mu$ s. Relevant standards (ISO, ANSI, FIPS) and Message Authentication Code (MAC) are fully supported. The use of the embedded DES co-processor increases execution speeds to a level where the actual time needed for a DES encryption becomes entirely irrelevant for an application. It also maximizes system security while enabling the system programmers to implement a highly advanced DES operation with minimum effort.

### 1.5 Security Features

SmartMX incorporates a range of security features to counter measure side channel attacks like DPA, SPA etc. Philips Semiconductors' deep knowledge of chip security, proven by the design of the WE-family and P8RF family, is now combined with Philips TANGRAM technology, the highly dense 0.18  $\mu$  five metal layer technology and Philips Glue logic methodology to make typical attack paths invalid. The effectiveness of the TANGRAM methodology has been proven on the MIFARE<sup>®</sup> ProX platform.

SmartMX's built in Memory Management Unit, which is designed to define various memory segments and assign security attributes accordingly, supports a strong firewall concept which keeps different applications separate from each other. Only a so-called system mode has full access privileges to all memory space and on-chip peripherals, while the user mode only has privileges defined upon card personalization and executed under the control of the system mode.

Philips Semiconductors will drive forward third party security evaluations to provide its customer with the relevant information and documentation needed to execute subsequent evaluations of implemented applications.

## Secure Smart Card Controller

## P5CC018

**1.6 PRODUCT TYPES**

The family members of the SmartMX **Contact and Contactless Security Controller** as well as SmartMX **Contact and Contactless PKI Controller** (Public Key Infrastructure via FameXE operation) are documented in a regularly updated Philips Semiconductors Identification "Product Line Sheet".

The naming scheme of the family can be described as follows:

<b>P5xyyy:</b>	<b>SmartMX Family</b>
with	
<b>xx = SC:</b>	Security Controller, ISO 7816 Contact Interface
<b>xx = CC:</b>	PKI Controller, ISO 7816 Contact Interface
<b>xx = SD:</b>	Security Controller, ISO 7816 Contact + ISO14443 Contactless Interface
<b>xx = CD:</b>	PKI Controller, ISO 7816 Contact + ISO14443 Contactless Interface
<b>xx = SU:</b>	Security Controller, ISO 7816 + USB 1.1 Contact Interface
<b>xx = CT:</b>	PKI Controller, ISO 7816 + USB 1.1 Contact + ISO14443 Contactless Interface
<b>xx = SR:</b>	Security Controller, ISO 14443 Contactless Interface
<b>xx = CR:</b>	PKI Controller, ISO14443 Contactless Interface
<b>yyy:</b>	Amount of Non-Volatile memory (EEPROM + optionally Flash) in Kbyte, increasing count for further product options.

**1.7 P5CC018 device**

The P5CC018 device includes 96 Kbytes of ROM, 4608 bytes of RAM (data memory) and 18 Kbytes of EEPROM, which can be used as data memory and as program memory. 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.

Bi-directional communication with the contact interface of the device can be performed through a serial interface IO. This IO is under full control of the application software in order to allow conditional controlled access to the different internal memories.

As all PKI family members of the Smart MX family the device provides a Memory Management Unit with functionality of a hardware firewall.

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

The P5CC018 provides two power saving modes with reduced activity: the IDLE and the SLEEP or CLOCKSTOP Mode. These two modes are activated by software.

The device operates either with a single 1.8V, 3 V or 5 V power supply at a maximum external clock frequency of 10 MHz supplied by the contact pads (internally up to 30MHz) or with a power supply generated from the electro magnetic field emitted by a reader antenna.

Operated in contact mode (ISO 7816) the user defines the final function of the card with his card operating system (COS). This allows the same level of security and flexibility for the contact interface.

Secure Smart Card Controller

P5CC018

2 BLOCK DIAGRAM

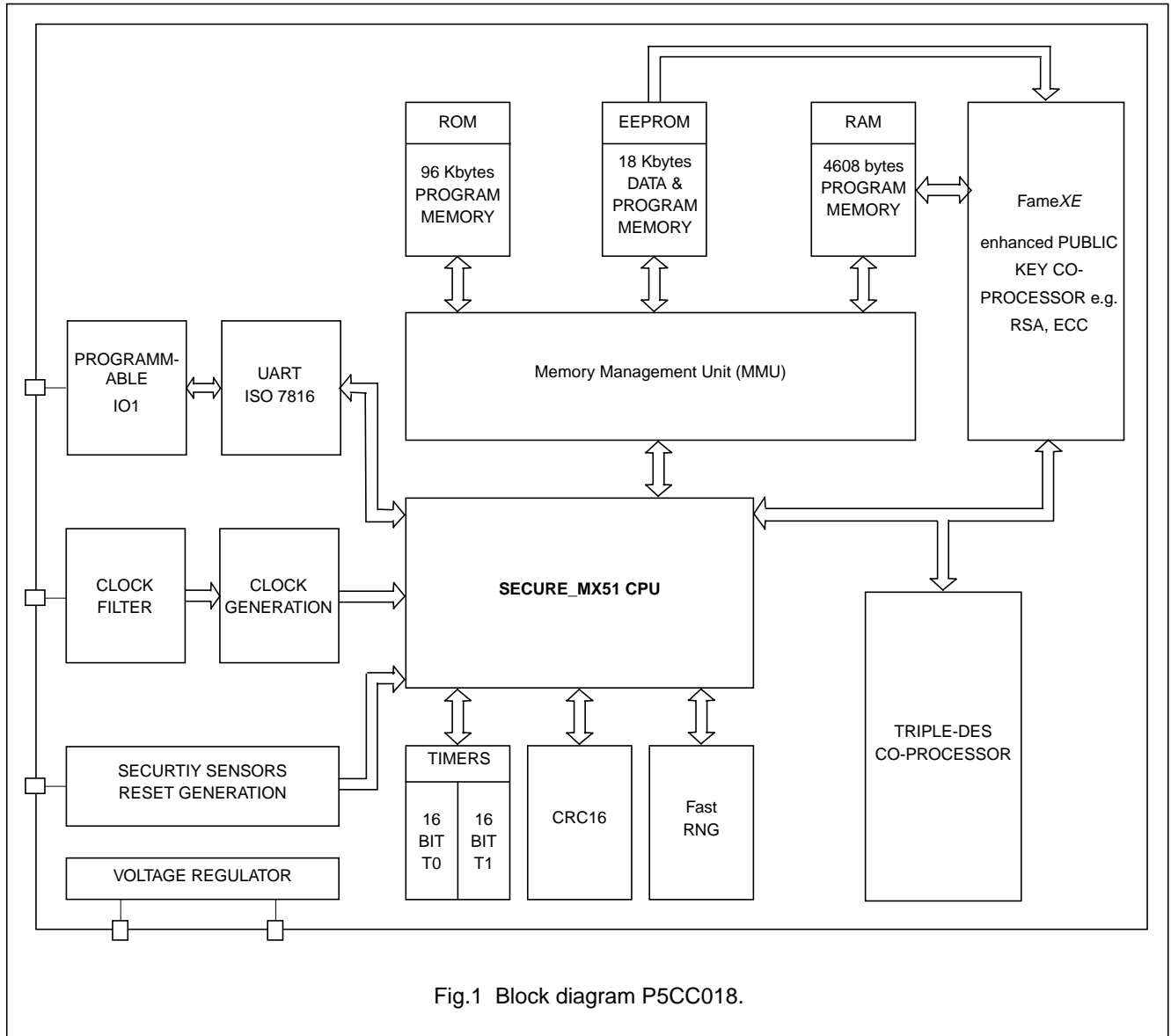


Fig.1 Block diagram P5CC018.

---

## Secure Smart Card Controller

## P5CC018

---

### 3 FEATURES

#### 3.1 Family Standard Features

- Secure\_MX51 CPU (**M**emory **eX**tended and enhanced 80C51) using 0.18  $\mu$  technology
  - operating in contact and contactless mode (dependent on family type option)
  - featuring a 24 bit universal memory space, 24 bit program counter
  - combined universal program/data linear address range up to 16 Mbyte
  - additional instructions to improve
    - pointer operations
    - performance and code density of both C and Java source code
  - Saving up to 30% memory space
- Developments/portation support to existing P8WE family mask (Compatibility Mode)
- Development/portation support to existing P8RF family masks
- Two 16-bit timers
- Multiple source vectorized interrupt system with four priority levels
- Error handling by customer defined exception interrupts
- Watch exception provides for software debugging facility
- 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 (temperature-dependent)
  - EEPROM data retention time: 10 years minimum
- Versatile EEPROM programming of 1 to 64 byte at a time
- Typical EEPROM page erasing time: 2 ms
- Typical EEPROM page programming time: 2 ms
- Power-saving IDLE Mode
  - Wake-up from IDLE Mode by RESET or any activated interrupt
- Power-saving SLEEP (power down) Mode or CLOCKSTOP Mode
  - Wake-up from SLEEP or CLOCKSTOP Mode by RESET or External Interrupt
- Contact configuration and serial interface according to ISO/IEC 7816: GND, VCC, CLK, RST, IO1
- ISO/IEC 7816 UART supporting standard protocols T=0 and T=1 as well as high speed personalisation at 1Mbit/s
- Low power / low voltage design using Philips TANGRAM technology
- External or internally generated configurable CPU clock
- 1 MHz to 10 MHz operating external clock frequency range
- Internal CPU clock up to 30 MHz with synchronous operation
  - Internal clocking independent of externally applied frequency
- High speed Triple-DES co-processor (three keys loadable), DES3 performance: < 50  $\mu$ s
- High speed 16 bit CRC Engine according to CCITT polynom definition
- Low power Random Number Generator (RNG) in hardware, FIPS140-2 compliant
- 1.62V to 5.5V extended operating voltage range for class A, B and C
- -25 to +85°C operating ambient temperature range

---

## Secure Smart Card Controller

## P5CC018

---

### 3.2 Security Features

- Power-up / Power-down reset
- Low / high supply voltage sensor
- Low / high clock frequency sensor
- Low / high temperature sensor
- Light sensor
- Single Fault Injection (SFI) attack detection
- EEPROM programming:
  - no external clock
  - hardware sequencer controlled
  - on-chip high voltage generation
- Electronic fuses for safeguarded mode control
- Unique serial number for each die
- 32 bytes Write Once Security area in EEPROM (bit access)
- 14 bytes User Write Protected Security area in EEPROM (byte access, inhibit functionality per byte)
- 32 bytes User Read Only area in EEPROM (byte access)
- 64 or 128 EEPROM bytes for customer-defined Security FabKey. Featuring batch-, wafer- or die-individual security data, incl. encrypted diversification features on request
- Clock Input Filter for protection against spikes
- Memory protection (encryption and physical measures) for RAM, EEPROM and ROM
- Customer specific EEPROM initialisation available
- *SmartConfig* Software for safe and reliable mask submission

### 3.3 Product Specific Features

- 18 Kbytes EEPROM (including 192 bytes reserved manufacturer/security area)
- 96 Kbytes User ROM
- 4608 bytes RAM
  - 256 bytes IRAM + 3 Kbytes XRAM
  - 1280 bytes FXRAM usable for FameXE
- Memory Management Unit (MMU) for:
  - memory mapping up to 8 Mbytes Code memory
  - memory mapping up to 8 Mbytes (-64 K) Data memory
  - secure multi application operating systems via two different operation modes
    - System Mode and User Mode
- Crypto Co-processor FameXE (**F**ast **A**ccelerator for **M**odular **E**xponentiation-**e**Xtended incl. **E**CC operations) optimized for public key cryptographic calculations and Elliptic Curve calculations
  - the major Public Key Cryptosystems like RSA, El'Gamal, DSS, Diffie-Hellmann, Guillou-Quisquater, Fiat-Shamir and Elliptic Curve are supported
  - 4096 bits maximum key length for RSA with randomly chosen modulus
  - 32-bit key length increments
  - boolean operations for acceleration of standard, symmetric cipher algorithms
  - Performance example: RSA Modular Exponentiation (Straight forward) < 25 ms (2048 bit key length and 18 bit exponent)

## Secure Smart Card Controller

## P5CC018

**3.4 Design-in Support**

- Approved Development Tool Chain
  - Keil PK51 development tool package incl. Vision2/dScopeC51 simulator, additional specific hardware drivers and ISO7816 interface board. A “SmartMX DBox” allows software debugging and integration tests. ([www.keil.com](http://www.keil.com))
  - Ashling Ultra-Emulator platform, stand alone ROM prototyping boards and ISO7816 card interface board. Code coverage and performance measurement software tools for real time software testing. ([www.ashling.com](http://www.ashling.com))
- Software Libraries
  - EEPROM Read / Write routines
  - Tutorial library with source code routines for all crypto co-processors DES and FameXE

**4 ORDERING INFORMATION****Table 1** Ordering Information of the P5CC018

TYPE NUMBER <sup>(1)</sup>	PACKAGE			TEMPERATURE RANGE (°C)
	NAME	DESCRIPTION		
P5CC018EAEW/0xxyyVz	FFC	sawn wafer 150 μ on film frame carrier	-	-25 to +85
P5CC018EAEV/0xxyyPz	Module	Module on super 35 mm film 8-contact	SOT658AA1	

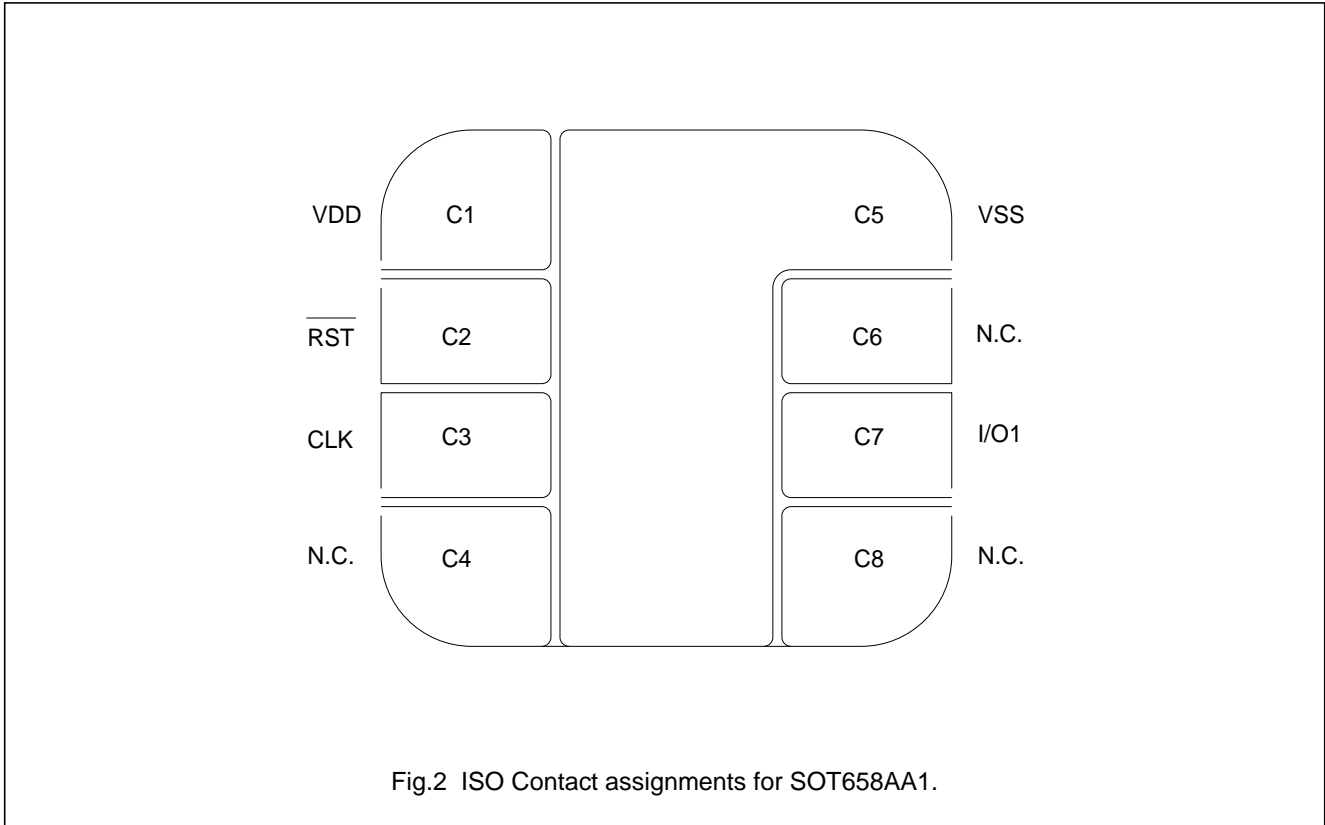
## Secure Smart Card Controller

## P5CC018

## 5 PINNING INFORMATION

## 5.1 Smart Card contacts

## 5.1.1 SMART CARD CONTACTS "STANDARD TYPE"



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

ISO 7816		STANDARD P5CC018	
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	IO	IO1	Input/Output #1 for serial data
C8	reserved	N.C.	not connected

# *Philips Semiconductors – a worldwide company*

## **Contact information**

For additional information please visit <http://www.semiconductors.philips.com>. Fax: **+31 40 27 24825**

For sales offices addresses send e-mail to: [sales.addresses@www.semiconductors.philips.com](mailto:sales.addresses@www.semiconductors.philips.com).

© Koninklijke Philips Electronics N.V. 2002

SCA74

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**