Security & Chip Card ICs

SLE 66C40S

16-bit Security Controller
in 0.6 µm CMOS Technology
32-Kbyte ROM, 1280 Byte RAM and
4-Kbyte EEPROM

Short Product Information 10.01

SLE 66C40S Short Product Information	Ref.: SPI_SLE 66C 40S_1001
This document contains preliminary information on a new product under development. Details are subject to change without notice.	
Revision History: Current Version 10.01	
Previous Releases:	
Page	Subjects (changes since last revision)

Important: Further information is confidential and on request. Please contact:
Infineon Technologies AG in Munich, Germany,
Security & Chip Card ICs,
Tel : +49 89 234-80000
Fax +49 89 234-81000
E-Mail: security.chipcard.ics@infineon.com

Edition 2001

Published by Infineon Technologies AG, CC Applications Group
St.-Martin-Strasse 53, D-81541 München

Attention please!

The information herein is given to describe certain components and shall not be considered as warranted characteristics.

Terms of delivery and rights to technical change reserved.

We hereby disclaim any and all warranties, including but not limited to warranties of non-infringement, regarding circuits, descriptions and charts stated herein.

Infineon Technologies is an approved CECC manufacturer.

Information

For further information on technology, delivery terms and conditions and prices please contact your nearest Infineon Technologies Office in Germany or our Infineon Technologies Representatives world-wide (see address list).

Warnings

Due to technical requirements components may contain dangerous substances. For information on the types in question please contact your nearest Infineon Technologies Office.

Infineon Technologies Components may only be used in life-support devices or systems with the express written approval of Infineon Technologies, if a failure of such components can reasonably be expected to cause the failure of that life-support device or system, or to affect the safety or effectiveness of that device or system. Life support devices or systems are intended to be implanted in the human body, or to support and/or maintain and sustain and/or protect human life. If they fail, it is reasonable to assume that the health of the user or other persons may be endangered.

16-bit Security Controller with 32-Kbyte ROM, 1280 Byte RAM and 4-Kbyte EEPROM

Features

- 16-bit microcomputer in 0.6 µm CMOS technology
- Instruction set opcode compatible with standard SAB 8051 processor
- Enhanced 16-bit arithmetic
- Additional powerful instructions optimized for chip card applications
- Dedicated, non-standard architecture with **execution time six times faster** than standard SAB 8051 processor
- **31.5-Kbytes User ROM** for application programs
- 512-bytes reserved ROM for Resource Management System (RMS) with intelligent write/erase routines
- **4-Kbytes EEPROM** as program/data memory
- **1280 bytes RAM**
- **True random number generator** (RNG)
- **Interrupt module for I/O interface**
- **CRC Module**
- **16-bit timer with 8-bit prescaler**
- Power saving sleep mode
- Clock freq. = int. freq.: 1 to 7.5 MHz
- Contact configuration and serial interface in accordance with ISO 7816
- Supply voltage range: 2.7 V to 5.5 V
- Current consumption < 10 mA at 5 MHz and 5.5 V
- Temperature range: -25 to +70°C
- ESD protection larger than 4 kV

Testmode

- Irreversible Lock - Out of testmode

EEPROM

- Reading, erasing and writing byte by byte
- Flexible page mode for 1 to 16 bytes write/erase operation
- 32 bytes security area
- Write time 3.62 ms, erase time 1.81 ms
- Programming time adaptable to clock frequency
- **Minimum of 500,000 write/erase cycles**
- Data retention for a minimum of ten years
- EEPROM programming voltage generated on chip

Security Features

Operation state monitoring mechanism

- Low and high voltage sensors
- Frequency sensors and filters

Memory Security

- 16 bytes security PROM, hardware protected
- Unique chip identification number for each chip
- MED – memory encryption/decryption device for XRAM, ROM and EEPROM
- True Random Number Generator with Firmware test function
- Security optimised layout and layout scrambling
- user settable additional encryption key for EEPROM
- Move code blocking (from EEPROM)

Support

- HW-& SW-Tools (Emulator, ROM Monitor, Card Emulator, Simulator, Softmasking)
- Application notes (e.g.: T=0, T=1, DES, RNG, etc.)

Anti Snooping

- HW-countermeasures against SPA/DPA-, Timing- and DFA-attacks (differential fault analysis – DFA)
- CRC - Module
- Non standard dedicated Smart Card CPU – Core

Development Tools Overview

- Short Product Information Software Development Kit SDK CC
- Short Product Information Card Emulator SCE66
- Short Product Information ROM Monitor SRM66
- Short Product Information Emulator SET66 Hitex or SET66 KSC
- Short Product Information Smart Mask Package

Supported Standards

- ISO/IEC 7816
- EMV 2000
- GSM 11.1x
- ETS I TS 102 221

Document References

- Confidential Data Book SLE 66CxxS
- Confidential Instruction SLE 66CxxS
- Confidential Quick Reference SLE 66CxxS
- Qualification report
- Chip delivery specification for wafer with chip-layout (die size, orientation,...)
- Module specification containing description of package, etc.
- Qualification report module

Ordering Information

Type	Package[1]	Voltage Range	Temperature Range	Frequency Range
SLE 66C40S	M4	2.7 V - 5.5 V	– 25°C to + 70°C	1 MHz - 5 MHz @ 5V 1 MHz - 4 MHz @ 3V
SLE 66C40S	C			
SLE 66C40S-T85	M4	2.7 V - 5.5 V	– 25°C to + 85°C	1 MHz - 5 MHz @ 5V 1 MHz - 4 MHz @ 3V
SLE 66C40S-T85	C			
SLE 66C40S-V5	M4	4.5 V - 5.5 V	– 25°C to + 70°C	1 MHz - 5 MHz
SLE 66C40S-V5	C			
SLE 66C40S-V5-T85	M4	4.5 V - 5.5 V	– 25°C to + 85°C	1 MHz - 5 MHz
SLE 66C40S-V5-T85	C			
SLE 66C40S-V5-F7	M4	4.5 V - 5.5 V	– 25°C to + 70°C	1 MHz - 7.5 MHz
SLE 66C40S-V5-F7	C			

[1] available as wire-bonded module (M4) for embedding in plastic cards or as die (C) for customer packaging

Pin Description

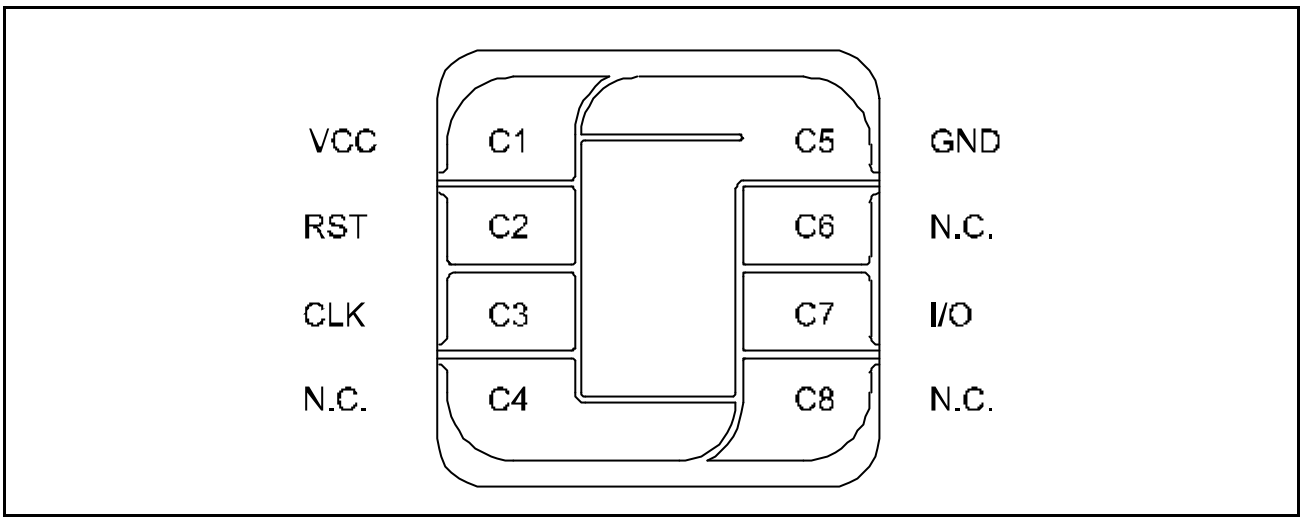

Figure 1 Pin Configuration (top view)

Pin Definitions and Functions

Card Contact	Symbol	Function
C1	VCC	Operating voltage
C2	RST	Reset input
C3	CLK	Processor clock input
C5	N.C.	Ground
C4; C6; C8	N.C.	Not connected
C7	I/O	Bi-directional-data-port

General Description

SLE 66C40S is a member of the Infineon Technologies high-end security controller family in 0.6 µm CMOS technology. The CPU provides the high efficiency of the SAB 8051-instruction set extended by additional powerful instructions together with enhanced performance, memory sizes and security features.

The controller IC offers 31.5 Kbytes of User-ROM, 256 bytes internal RAM, 1 Kbyte XRAM and 4 Kbytes EEPROM. It suits the requirements of the new generation of operating systems.

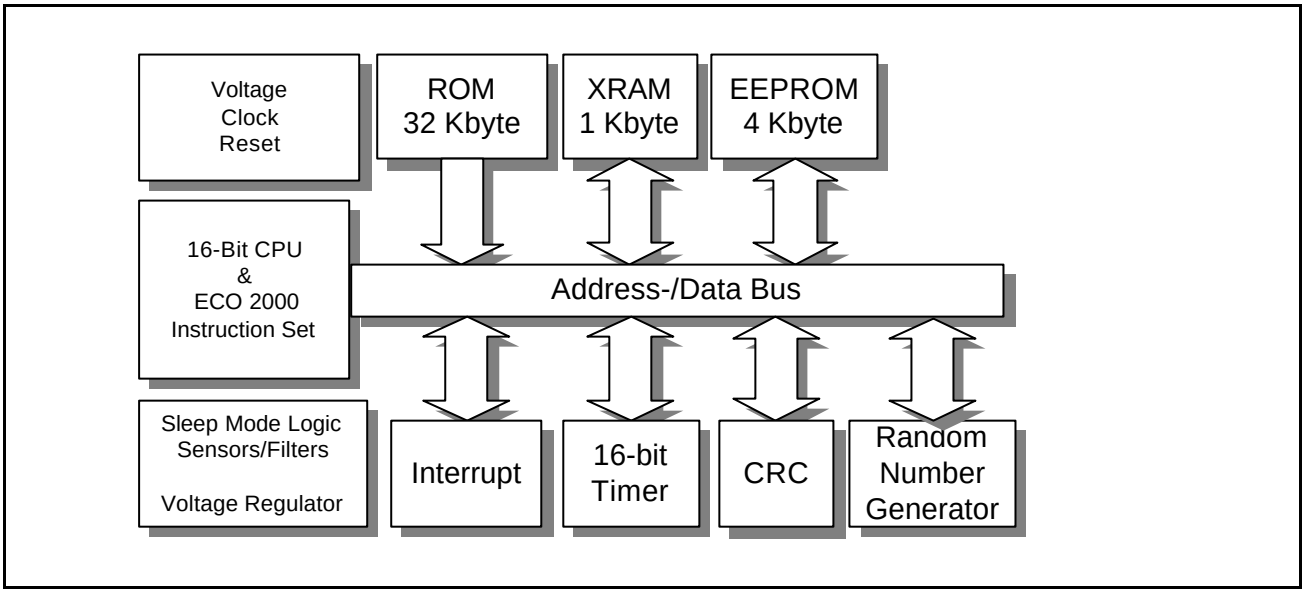

Figure 2: Block Diagram SLE 66C40S

The random number generator (RNG) is able to supply the CPU with true random numbers on all conditions. The CRC module allows the easy generation of checksums according to ISO 3309 (16-Bit-CRC). The timer makes it easy to implement advanced communication protocols such as T=1 and all other time critical processes. An additional interrupt capability of the I/O module allows parallel operation of chip card and terminal. To minimize the overall power consumption, the chip card controller IC offers a sleep mode.

As an important measure, the chip provides a new and enhanced level of on-chip security features.

In conclusion, the SLE 66C40S fulfills the requirements of all chip card applications, as especially SIM Cards for GSM Phones, payment, Health Care, Pay-TV and Access Control. The SLE 66C40S is a powerful chip card controller IC integrating outstanding memory sizes, additional peripherals in combination with enhanced performance and optimized power consumption on a minimized die size. Therefore, the SLE 66C40S offers the basis for new chip card applications.