Security & Chip Card ICs

SLE 66C640P

16-Bit Security Controller
with Memory Management and Protection Unit
in 0.22 µm CMOS Technology
136-Kbytes ROM, 4352 bytes RAM, 64-Kbytes EEPROM

Short Product Information 08.01

SLE 66C640P Short Product Information	Ref.: SPI SLE 66C640P 0801.doc
This document contains preliminary information on a new product under development. Details are subject to change without notice.	
Revision History: Current Version 08.01	
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 - (0)89 234-80000
Fax +49 - (0)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 MMU in 0.22µm CMOS Technologie
136 Kbytes ROM, 4352 bytes RAM, 64 Kbytes EEPROM

Features

- 16-bit microcomputer in 0.22 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 6 times faster (18 times by PLLmax)** than standard SAB 8051 processor at external same clock
- **134 Kbytes User ROM** for application programs
- Additional 2 Kbytes reserved ROM for Resource Management System (RMS+ light) with intelligent EEPROM write/erase routines
- **64 Kbytes Slim-EEPROM**
- **4 Kbytes** XRAM, 256 Bytes IRAM
- **Memory Management and Protection Unit (MMU)**
- CRC Module
- Interrupt Module
- Two 16-bit Autoreload Timer
- **PLL**
- Power saving sleep mode
- **External clock frequency 1 to 7.5 MHz for internal clock £ 10 MHz**
- **UART for handling serial interface** in accordance with ISO/IEC 7816 part 3 **supporting transmission protocols T=1 and T=0**
- I/O routines realized in software executable
- Supply voltage range: 2.7 V to 5.5 V
- Current consumption

< 10mA @ 5.5 V
< 6 mA @ 3.3 V

- Temperature range: -25 to +85°C
- ESD protection larger than 6 kV

Slim-EEPROM

- Reading, erasing and writing byte by byte
- Flexible page mode for 1 to 64 bytes write/erase operation
- 32 bytes security area (OTP)
- Fast personalization mode
- Erase + Write time < 4.5 ms
- **Minimum of 500.000 write/erase cycles at 25°C**
- Data retention for a minimum of 10 years
- EEPROM programming voltage generated on chip

Memory Management and Protection Unit

- Addressable memory up to 1 Mbyte
- Separation OS (system) and application (user)
- System routines called by traps
- OS can restrict access to peripherals in application mode
- Code execution from XRAM possible

Security Features

Operation state monitoring mechanism

- Low and high voltage sensors
- Frequency sensors and filters
- Glitch Sensor

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

Testmode

- Irreversible Lock - Out of testmode

Anti Snooping

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

Support

- HW-& SW-Tools (Emulator, ROM Monitor, Card Emulator, Simulator, Softmasking)
- Application notes

Supported Standards

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

Document References

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

Development Tools Overview

- Short Product Information Software Development Kit SDK CC
- Short Product Information Card Emulator CE66P
- Short Product Information ROM Monitor RM66P
- Short Product Information Emulator ET66P Hitex or ET66P KSC
- Short Product Information Smart Mask Package

Ordering Information

Type	Package[1]	Voltage Range	Temperature Range	Frequency Range (ext. clock frequency)
SLE 66C640P M5	M5	2.7 V - 5.5 V	– 25°C to + 70°C	1 MHz - 5 MHz
SLE 66C640P C	die			
SLE 66C640P-T85 M5	M5	2.7 V - 5.5 V	– 25°C to + 85°C	1 MHz - 5 MHz
SLE 66C640P-T85 C	die			
SLE 66C640P-F7 M5	M5	2.7 V - 5.5 V	– 25°C to + 70°C	1 MHz – 7.5 MHz
SLE 66C640P-F7 C	die			

Production sites:

- Dresden SLE66CxxxP
- UMC Taiwan SLE66CxxxPU

[1] available as wire-bonded module (M5) for embedding in plastic cards or as die (C) for customer packaging

Pin Configuration

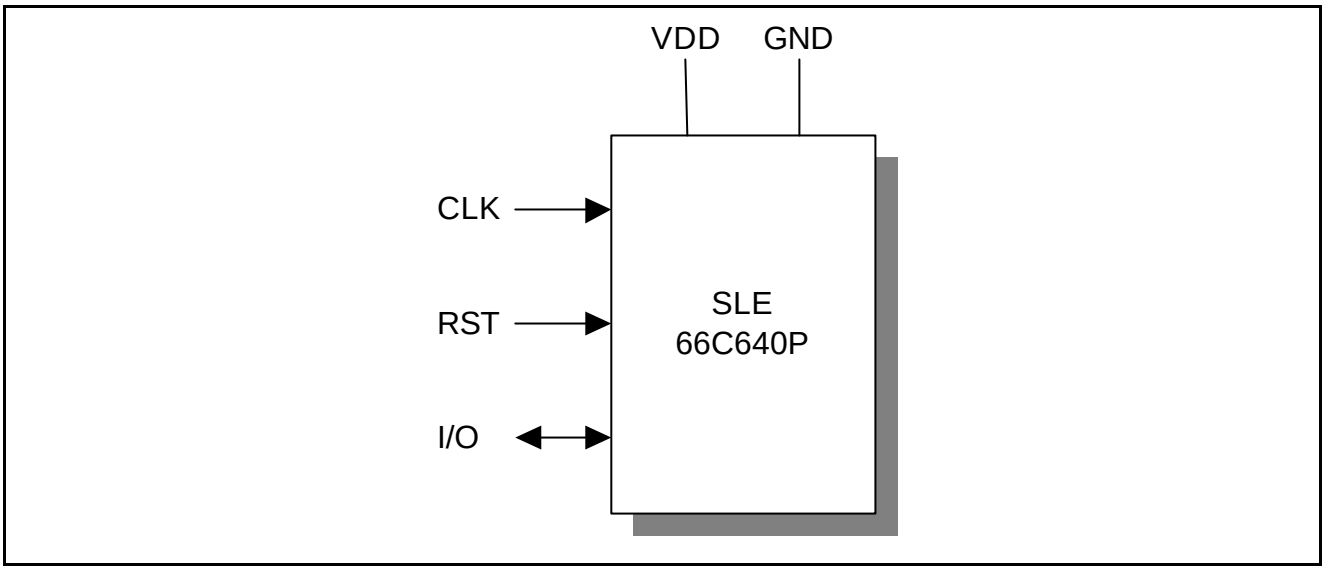

Figure 1: Pin Configuration

Pin Definitions and Functions

Symbol	Function
VCC	Operating voltage
RST	Reset input
CLK	Processor clock input
GND	Ground
I/O	Bi-directional data port

General Description

SLE 66C640P is another member of Infineon Technologies high-end security controller family in advanced 0.22 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 internal clock frequency can be adjusted up to 10 MHz independent of the clock rate of the terminal with the help of the PLL.

The controller IC offers 134 Kbytes of User-ROM, 256 bytes internal RAM, 4096 bytes XRAM and 64 Kbytes Slim-EEPROM. The Memory Management and Protection Unit allows a secure separation of the operating system and the applications. Furthermore the MMU makes a secure downloading of applications possible after the personalization of a card. These new features meet the requirements of the next generation of multi application operating systems. For code compatibility to the SLE 66CxxS family, a transparent mode for the MMU is available which allows you to keep the memory mapping of the SLE 66CxxS products.

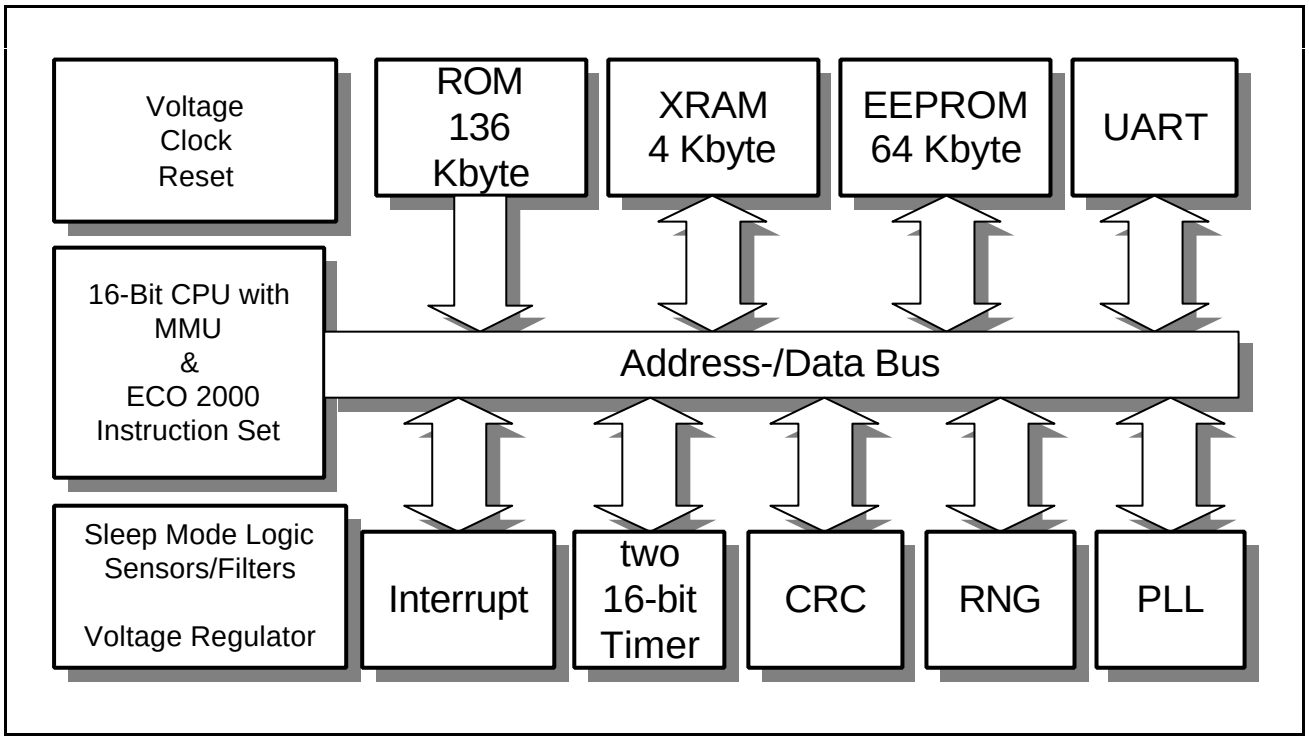

Figure 2: Block Diagram SLE 66C640P

The CRC module allows the easy generation of checksums according to ISO/IEC 3309 (16-Bit-CRC). To minimize the overall power consumption, the chip card controller IC offers a sleep mode. The UART supports the half-duplex transmission protocols T=0 and T=1 according to ISO/IEC 7816-3. All relevant transmission parameters can be adjusted by software, as e.g. the clock division factor, direct/inverse convention and the number of stop bits. Additionally, the I/O port can be driven by communication routines realized in software.

The random number generator (RNG) is able to supply the CPU with true random numbers under all conditions.

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

In conclusion, the SLE 66C640P fulfills the requirements of today's chip card applications, as GSM, and offers a powerful platform for future multi application cards. The SLE 66C640P integrates outstanding memory sizes, additional peripherals in combination with enhanced performance and optimized power consumption on a minimized die size. Therefore, the SLE 66C640P offers the basis for a generation of new chip card applications.