Security & Chip Card ICs

SLE 66CX640P

16-Bit Security Controller
with Memory Management and Protection Unit
in 0.25 µm CMOS Technology
136-Kbyte ROM, 5052 bytes RAM, 64-Kbyte EEPROM
1100-Bit Advanced Crypto Engine and
112-Bit/ 192-Bit DDES EC2 Accelerator

Short Product Information 08.01

SLE 66CX640P Short Product Information	Ref.: SPI_SLE66CX640P_0801doc
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: 03.00	
Page	Subjects (changes since last revision)
3	RMS size corrected from 2 Kbytes to 1 Kbytes

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

© Infineon Technologies AG 2001
All Rights Reserved.

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 0.25µm CMOS Technology 136-Kbyte ROM, 5052 bytes RAM, 64-Kbyte EEPROM 1100-Bit Advanced Crypto Engine and 112-Bit/ 192-Bit DDES Accelerator

Features

- 16-bit microcomputer in 0.25 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 same external clock
- **135 Kbytes User ROM** for application programs
- Additional 1 Kbytes reserved ROM for Resource Management System (RMS+) with intelligent EEPROM write/erase routines
- **64 Kbytes EEPROM**
- **4 Kbytes** XRAM, 256 (+700) bytes internal RAM
- **Memory Management and Protection Unit (MMU)**
- **Dual Key Triple DES (DDES) and EC2 GF (2^n) Accelerator**
- **Advanced Crypto Engine for up to 2048 bit RSA computation**
- CRC Module
- Interrupt Module
- **PLL**
- Two 16-bit Autoreload Timer
- Power saving sleep mode
- **Ext. Clock freq. 1 to 7.5 MHz for int. 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
- ESD protection larger than 6 kV

EEPROM

- Reading, erasing and writing byte by byte
- Flexible page mode for 1 to 64 bytes write/erase operation
- 32 bytes security area (OTP)
- 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
- Separates 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

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

- Current consumption
< 10mA @ 5.5 V
< 6 mA @ 3.3 V
- Temperature range: -25 to +85°C

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
- Active Shield with automatic and user controlled attack detection

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

Performance Advanced Crypto Engine

Operation	Modulus	Exponent	Calculation Time		
			5MHz	10 MHz	15 MHz
Modular Exponentiation RSA Encrypt / RSA Signature Verify	1024 bit	17 bit	20 ms	11 ms	7 ms
Modular Exponentiation RSA Decrypt / RSA Signature Generate	1024 bit	1024 bit	820 ms	410 ms	273 ms
Modular Exponentiation using CRT RSA Decrypt / RSA Signature Generate	Eq.1024 bit	eq.1024 bit	250 ms	125 ms	83 ms
DSA Signature Generate	512 bit	160 bit	97ms	49 ms	32 ms
DSA Signature Verify	512 bit	160 bit	117 ms	59 ms	39 ms
DSA Signature Generate	1024 bit	160 bit	438 ms	219 ms	146 ms
DSA Signature Verify	1024 bit	160 bit	711 ms	356 ms	237 ms

Performance DDES-EC2 Accelerator

Operation	Data Block Length	Encryption Time for an 8-Byte Block incl. Data Transfer		
		5 MHz	10 MHz	15 MHz
56-bit Single DES Encryption	64 bit	23 µs	11 µs	8 µs
112-bit Triple DES Encryption	64 bit	35 µs	17 µs	12 µs
	Operand Length	**Calculation Time**		
		5 MHz	**10 MHz**	**15 MHz**
Elliptic Curves GF(2^n) EC-DSA Signature Generate	192 bit	285 ms	142 ms	95 ms
Elliptic Curves GF(2^n) EC-DSA Signature Verify	192 bit	540 ms	270 ms	180 ms

Ordering Information

Type	Package[1]	Voltage Range	Temperature Range	Frequency Range (ext. clock frequency)
SLE 66CX640P M5	M5	2.7 V - 5.5 V	– 25°C to + 70°C	1 MHz - 5 MHz
SLE 66CX640P C	Die			
SLE 66CX640P-T85 M5	M5	2.7 V - 5.5 V	– 25°C to + 85°C	1 MHz - 5 MHz
SLE 66CX640P-T85 C	Die			
SLE 66CX640P-F7 M5	M5	2.7 V - 5.5 V	– 25°C to + 70°C	1 MHz – 7.5 MHz
SLE 66CX640P-F7 C	die			

Production sites:

- Dresden SLE 66CxxxP
- UMC Taiwan SLE 66CxxxPU

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

Pin Configuration

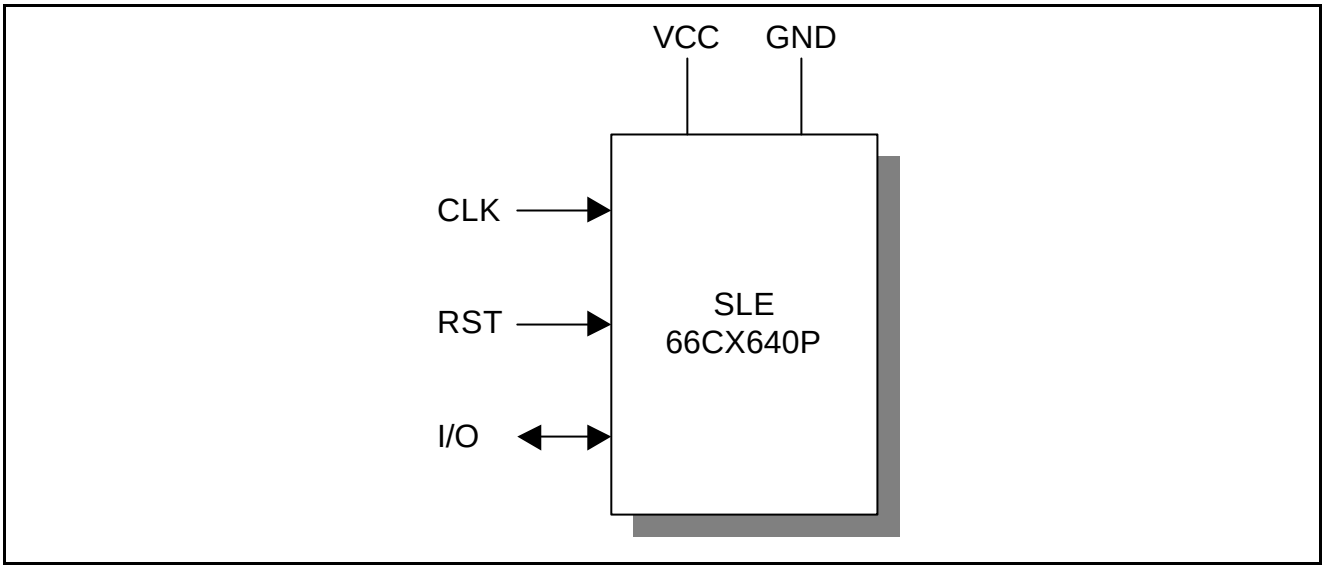


Figure 1: Pin Configuration

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 66CX640P is another member of Infineon Technologies high end security controller family in advanced 0.25 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 15 MHz independent of the clock rate of the terminal with the help of the PLL.

The controller IC offers 135 Kbytes of User-ROM, 256 byte internal RAM, 4096 byte XRAM and 64 Kbytes 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 suit 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 established which allows to keep the memory mapping of the SLE 66CxxS products.

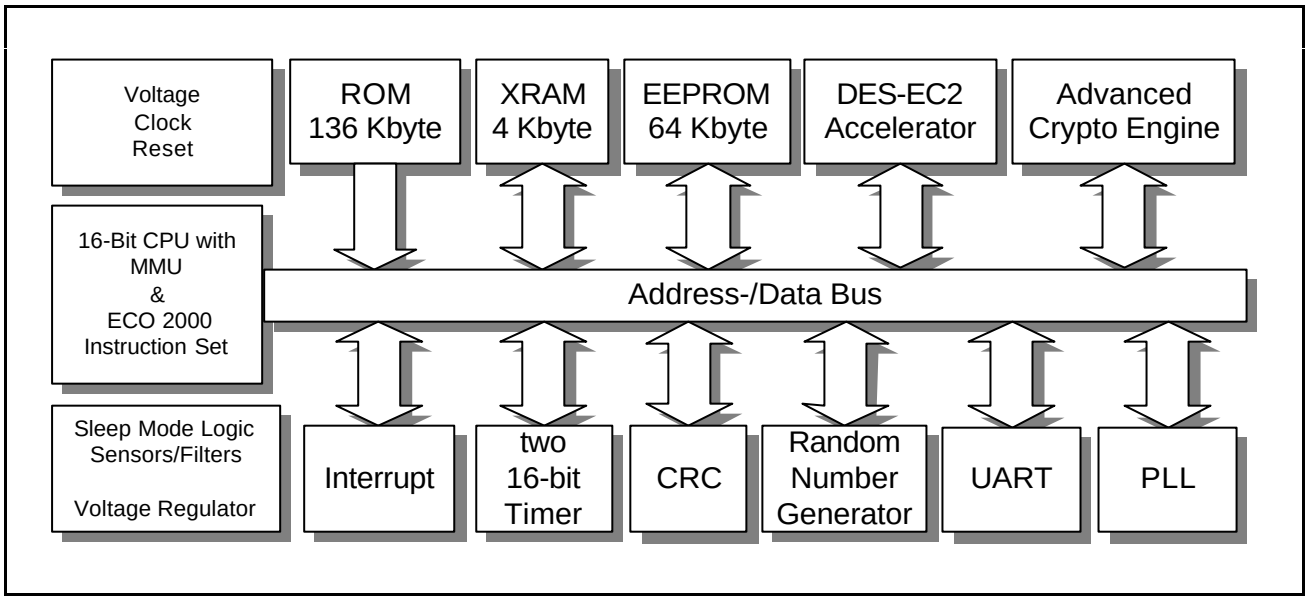


Figure 2: Block Diagram SLE 66CX640P

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 Advanced Crypto Engine is equipped with its own RAM of 700 bytes and supports all of today known public-key algorithms based on large integer modular arithmetic. It allows fast and efficient calculation of e.g. RSA operations with key lengths up to 2048 bit.

The DDES-EC2 accelerator consists of two modules. The DES module supports symmetrical crypto algorithms according to the Data Encryption Standard in the Electronic Code Book Mode. The EC2 module accelerates the multiplication in $GF(2^n)$ and therefore the operations for elliptic curve cryptography.

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

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

In conclusion, the SLE 66CX640P fulfills the requirements of today's chip card applications, such as payment, GSM, Pay TV, security access and digital signature and offers a powerful platform for future multi application cards. The SLE 66CX640P integrates outstanding memory sizes, additional peripherals in combination with enhanced performance and optimized power consumption on a minimized die size. Therefore, the SLE 66CX640P offers the basis for a generation of new chip card applications.