preliminary

# Security & Chip Card ICs

# SLE 66CX642P

16-Bit Security Controller
with Memory Management and Protection Unit
in 0.22 µm CMOS Technology
208-Kbytes ROM, 5052 bytes RAM, 64-Kbytes EEPROM
1100-Bit Advanced Crypto Engine and
112-Bit / 192-Bit DDES-EC2 Accelerator

Short Product Information 11.02

| SLE 66CX642P Short Product Information | Ref.: SPI_SLE 66CX642P_1102.doc |
|---|---|
| **This document contains preliminary information on a new product under development. Details are subject to change without notice.** | |
| **Revision History: Current Version 11.02** | |
| Previous Releases: 04.02 | |
| Page | 3,6 |
| | |

***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 2002

**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 Technology 208-Kbytes ROM, 5052 bytes RAM, 64-Kbytes EEPROM 1100-Bit ACE and 112-Bit / 112-Bit / 192-Bit DDES-EC2 Accelerator

## 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 same external clock
- **206 Kbytes User ROM** for application programs
- Additional 2 Kbytes reserved ROM for Resource Management System (RMS+ Superslim) with intelligent EEPROM write/erase routines
- **64 Kbytes Superslim-EEPROM**
- **4 Kbytes** XRAM, 256 (+ 700) Bytes IRAM
- **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**
- **Certified RSA 2048 library** available (refer to product brief)
- CRC Module
- Interrupt Module
- Two 16-bit Autoreload Timer
- **PLL** up to 15 MHz
- Power saving sleep mode
- **Ext. Clock freq. 1 to 7.5 MHz for int. Clock £ 15 MHz @ 2.7V-5.5V**
  **Ext. Clock freq. 1 to 5 MHz for int. Clock £ 11 MHz @ 1.62V-5.5V**
- **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: 1.62 V to 5.5 V
- Current consumption
  < 10mA @ 5.5 V
  < 6 mA @ 3.3 V
  < 4 mA @ 1.98 V
- Temperature range: -25 to +85°C
- ESD protection larger than 6 kV

## Superslim-EEPROM

- Reading and programming byte by byte
- Flexible page mode for 1 to 64 bytes write/erase operation
- 32 bytes security area (OTP)
- Fast personalization mode 0.63 ms @15MHz
- Erase + Write time < 4.0 ms @15MHz
- **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
- Light Sensor
- Glitch Sensor
- Temperature Sensor
- Life Test Function for Sensors

### 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 11.11, 11.12, 11.18
- ETS I TS 102 221

### 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

### Document References

- Confidential Data Book SLE66CxxxP
- 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 Info Software Development Kit SDK CC
- Short Product Info Card Emulator CE66P
- Short Product Info ROM Monitor RM66P
- Short Product Info Emulator ET66P Hitex or ET66P KSC
- Short Product Info Smart Mask Package

**Performance Advanced Crypto Engine**

| Operation | Modulus | Exponent | Calculation Time | | |
|---|---|---|---|---|---|
| | | | 5MHz | 10 MHz | 15 MHz |
| Modular Exponentiation<br>RSA Encrypt / RSA Signature Verify | 1024 bit<br>2048 bit | 17 bit<br>17 bit | 20 ms<br>630 ms | 11 ms<br>315 ms | 7 ms<br>210 ms |
| Modular Exponentiation<br>RSA Decrypt / RSA Signature Generate | 1024 bit | 1024 bit | 820 ms | 410 ms | 273 ms |
| Modular Exponentiation using CRT<br>RSA Decrypt / RSA Signature Generate | eq.1024 bit<br>eq.2048 bit | eq.1024 bit<br>eq.2048 bit | 250 ms<br>1840 ms | 125 ms<br>920 ms | 83 ms<br>614 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 | 10MHz | 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 66CX642P M5 | M5 | 2.7 V - 5.5 V<br>or<br>1.62 V – 5.5 V | – 25°C to + 70°C<br>or<br>– 25°C to + 85°C | 1 MHz - 5 MHz<br>or<br>1 MHz - 7.5 MHz |
| SLE 66CX642P C | Die | | | |

For ordering information please refer to the databook and contact your sales representative.

**Production sites:**

- Dresden (Germany) SLE 66CxxxP
- UMC (Taiwan) SLE 66CxxxPU
- Altis (France) SLE 66CxxxPA

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

## Pin Configuration

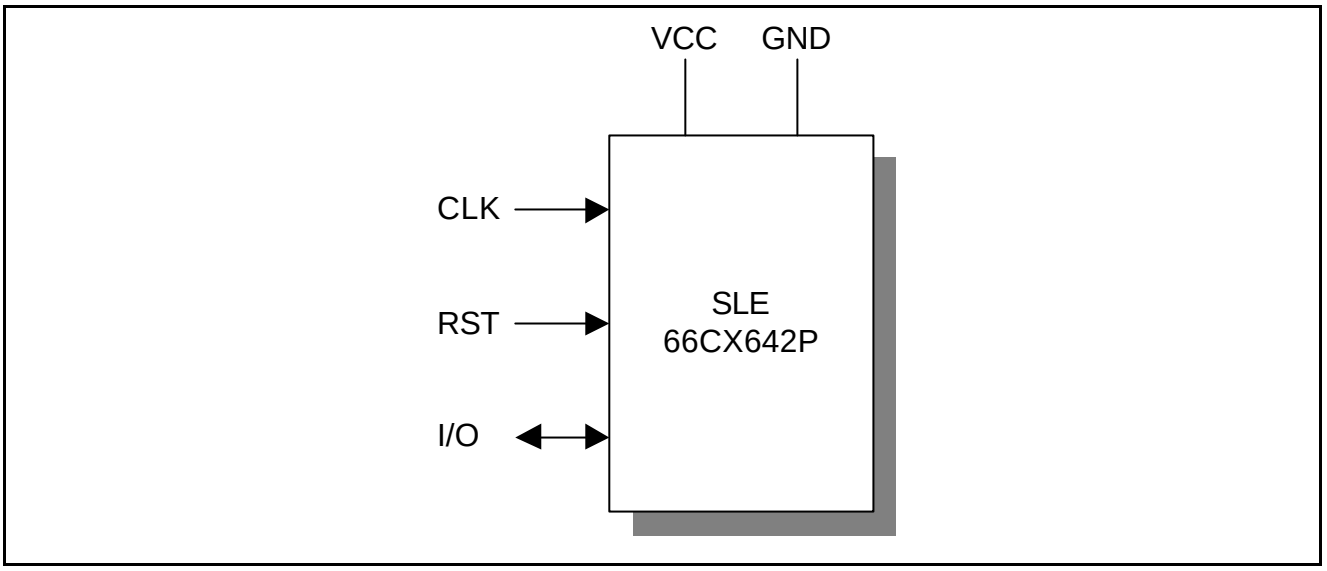


**Figure 1: Pin Configuration**

## 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 66CX642P is a 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 15 MHz independent of the clock rate of the terminal with the help of the PLL.

The controller IC offers 206 Kbytes of User-ROM, 256 byte internal RAM, 4096 byte XRAM and 64 Kbytes Superslim-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.

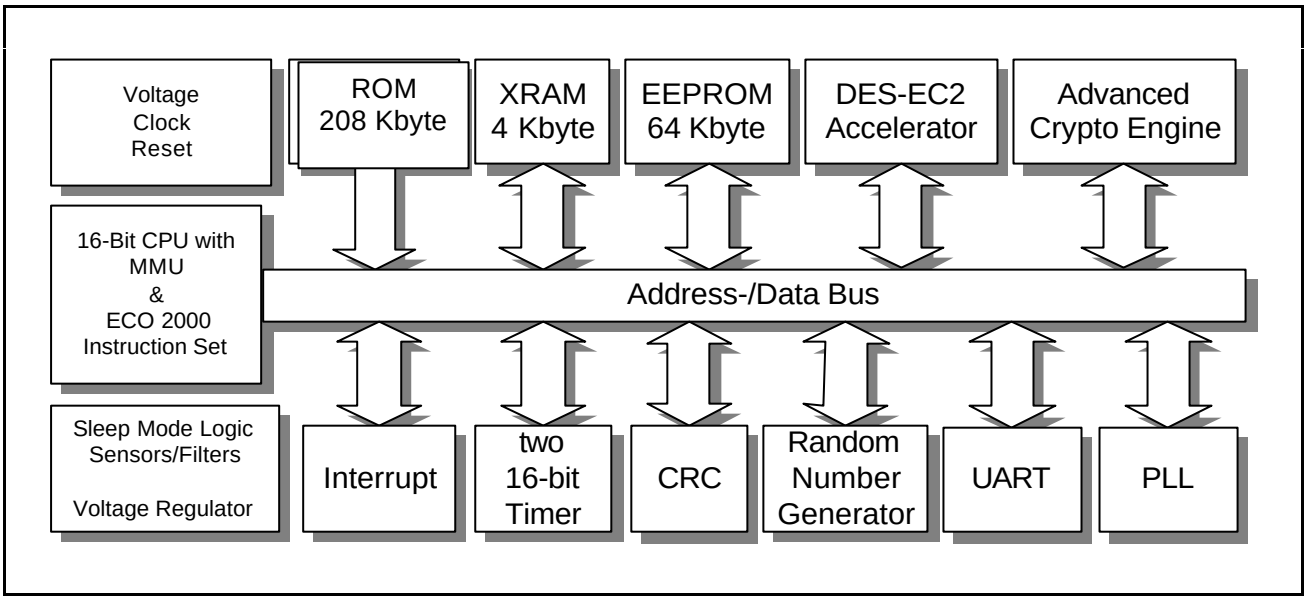


**Figure 2: Block Diagram SLE 66CX642P**

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, which fulfills the strong security requirements of a Common Criteria evaluation at an EAL5 level.

In conclusion, the SLE 66CX642P fulfills the requirements of today's chip card applications, such as payment, GSM, UMTS, Pay TV, security access and digital signature and offers a powerful platform for future multi application cards. The SLE 66CX642P integrates outstanding memory sizes, additional peripherals in combination with enhanced performance and optimized power consumption on a minimized die size. Therefore, the SLE 66CX642P offers the basis for a generation of new chip card applications.