



## Security & Chip Card ICs

### SLE 66C82P

16-Bit Security Controller

with Memory Management and Protection Unit

in 0.22  $\mu\text{m}$  CMOS Technology

64-Kbyte ROM, 2304 bytes RAM, 8-Kbyte EEPROM

112-Bit / 192-Bit DDES-EC2 Accelerator

**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: 0202

| Page | Subjects (changes since last revision) |
|------|--|
|------|--|

|     |  |
|-----|--|
| 3,4 |  |
|-----|--|

**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 2002

**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 0.22 $\mu\text{m}$ CMOS Technology

### 64-Kbyte ROM, 2304 bytes RAM, 8-Kbyte EEPROM

### 112-Bit / 192-Bit DDES-EC2 Accelerator

#### Features

- 16-bit microcomputer in 0.22  $\mu\text{m}$  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
- **62 Kbytes User ROM** for application programs
- Additional 2 Kbytes reserved ROM for Resource Management System (RMS+ Superslim) with intelligent EEPROM write/erase routines
- **8 Kbytes Superslim-EEPROM**
- **2 Kbytes XRAM**, 256 Bytes IRAM
- **Memory Management and Protection Unit (MMU)**
- **Dual Key Triple DES (DDES) and EC2 GF (2<sup>n</sup>) Accelerator**
- CRC Module
- Interrupt Module
- Two 16-bit Autoreload Timer
- **PLL up to 15 MHz**
- Power saving sleep mode
- **External clock frequency 1 to 7.5 MHz for internal clock  $\leq$  15 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**

#### 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
- Erase + Write time < 4.0 ms @ 15 MHz
- **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 96
- GSM 11.11, 11.12, 11.18
- ETSI 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
- user settable additional encryption key for EEPROM

**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

**Features (cont'd)**
**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 Exponentiation                              | 64 bit            | 23 $\mu$ s  | 11 $\mu$ s | 8 $\mu$ s  |
| 112-bit Triple DES Exponentiation                             | 64 bit            | 35 $\mu$ s  | 17 $\mu$ s | 12 $\mu$ s |
|   | Operand Length    | Calculation Time  |            |            |
|   |                   | 5 MHz   | 10 MHz     | 15 MHz     |
| Elliptic Curves GF(2 <sup>n</sup> ) EC-DSA Signature Generate | 192 bit           | 285 ms  | 142 ms     | 95 ms      |
| Elliptic Curves GF(2 <sup>n</sup> ) EC-DSA Signature Verify   | 192 bit           | 540 ms  | 270 ms     | 180 ms     |

**Ordering Information**

| Type          | Package <sup>1</sup> | Voltage Range        | Temperature Range      | Frequency Range (ext. clock frequency) |
|---------------|----------------------|----------------------|------------------------|--|
| SLE 66C82P M5 | M5                   | 2.7 V - 5.5 V        | - 25°C to + 70°C       | 1 MHz - 5 MHz                          |
| SLE 66C82P C  | Die                  | or<br>1.62 V - 5.5 V | or<br>- 25°C to + 85°C | or<br>1 MHz - 7.5 MHz                  |

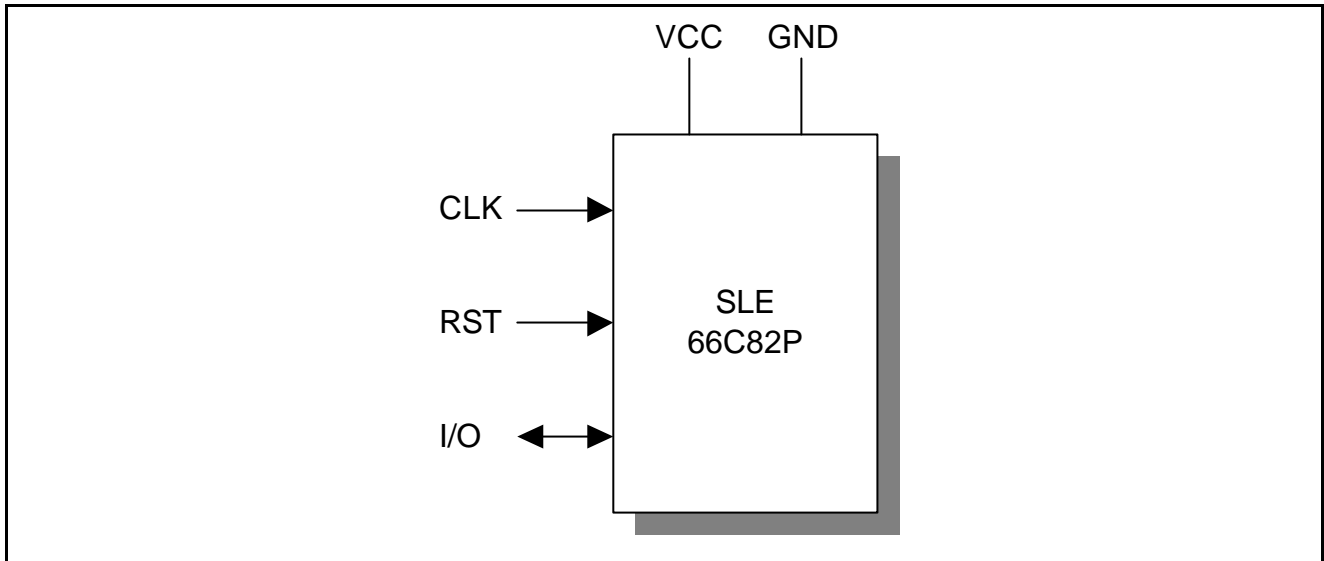
For ordering information please refer to the databook and contact your sales representative.

**Production sites:**

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

<sup>1</sup> available as wire-bonded module (M5) for embedding in plastic cards or as die (C) for customer packaging

**Pin Configuration**



**Figure 1: Pin Configuration**

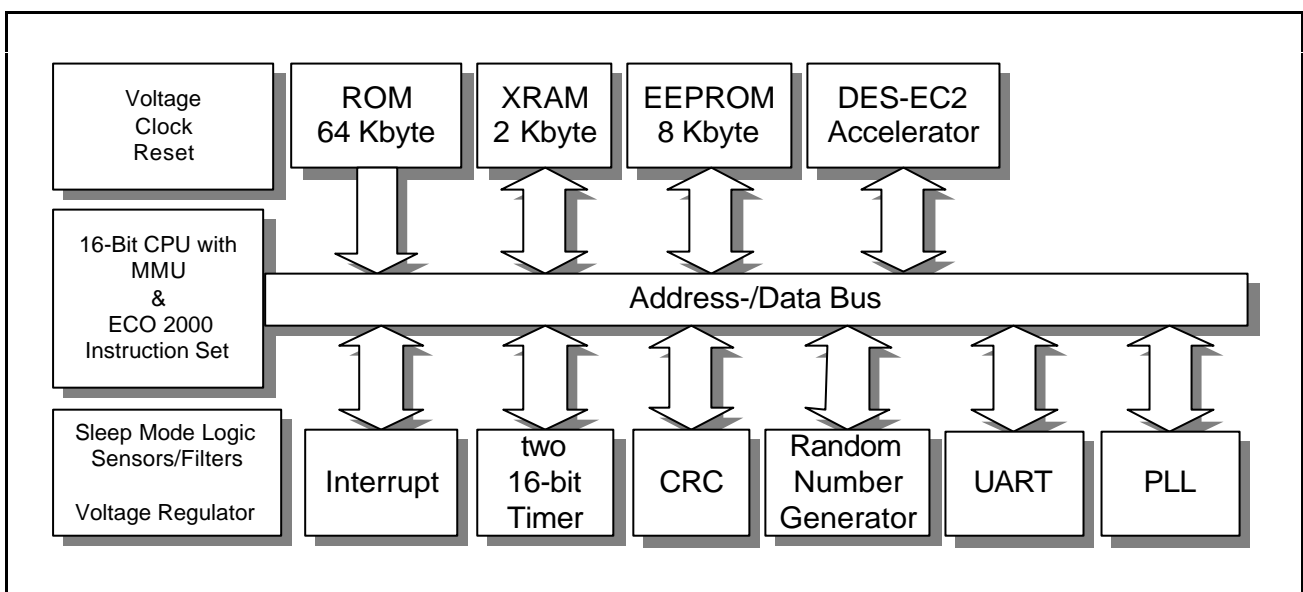
**Pin Definitions and Functions**

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

**General Description**

SLE 66C82P is another member of Infineon Technologies high-end security controller family in advanced 0.22  $\mu\text{m}$  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 62 Kbytes of User-ROM, 256 bytes internal RAM, 2 Kbytes XRAM and 8 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 66C82P**

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 on all conditions.

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.

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

In conclusion, the SLE 66C82P fulfills the requirements of today's chip card applications, as GSM and payment.