Chip Card & Security ICs

SLE 66CX480PE

48 Kbyte EEPROM
244 Kbyte ROM
7100 bytes RAM
1100-bit Advanced Crypto Engine
  certified RSA 2048-bit library available
Dual Key Triple DES

8/16-Bit Security Controller with enhanced instruction set for large memories in 0.22 µm CMOS Technology

Preliminary

Short Product Information 03.06

SLE 66CX480PE Short Product Information	Ref.: SPI_SLE66CX480PE_0306
This document contains preliminary information on a new product under development. Details are subject to change without notice.	
Revision History: Current Version 03.06	
Previous Releases:	
Page	

Important: Further information is confidential and on request. Please contact:
Infineon Technologies AG in Munich, Germany,
Chip Card & Security ICs,
Tel +49 - (0)89 234-80000
Fax +49 - (0)89 234-81000
E-Mail: security.chipcard.ics@infineon.com

Published by Infineon Technologies AG, CC
81726 Munich, Germany

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.

8/16-Bit Security Controller with enhanced instruction set for large memories in 0.22µm CMOS Technology
244-Kbyte ROM, 7100 bytes RAM, 48-Kbyte EEPROM
1100-Bit ACE and Dual Key Triple DES Accelerator

General Features

- 8/16-bit microcontroller in 0.22 µm CMOS technology
- Instruction set opcode compatible with standard SAB 8051 processor
- **Downward compatibility to existing SLE66CxxxP products for existing masks (without using the new features)**
- **Addressable memory up to 16 Mbyte**
- **Additional enhanced instructions for direct physical memory access of >64kByte**
  - Typically saves up to 90 % code space and increases execution speed up to 80%.
- Dedicated, non-standard architecture with **execution time 6 times faster** than standard SAB 8051 processor at same external clock. (Up to **18 times faster** using internal frequency PLL x 3 compared to external clock)
- **244-Kbytes User ROM** for application programs
- **48-Kbytes MicroSlim-EEPROM** for increased memory requirements in mobile applications
- **6-Kbytes XRAM,** 256 bytes internal RAM, 700 bytes Crypto RAM.
- **Enhanced Memory Management and Protection Unit (MMU)** with application and user defined segments
- **Dual Key Triple DES (DDES)**
- **Advanced Crypto Engine:**
  - **Up to 1100 bit RSA calculation in Hardware**
  - **Up to 2048 bit RSA calculation via fast and secure RSA 2048 crypto library** (CC EAL 5+ certified – refer to product brief)
  - **Supports Elliptic Curves over GF(p)**
- CC EAL5+ certification according to BSI-PP-0002 planned
- True Random Number Generator with Firmware test function; AIS-31 compliant
- CRC Module
- 16-bit Interrupt Module
- Code executions during E²-programming for faster personalization
- EEPROM programming voltage generated on chip
- **Internal Clock** with up to 33 MHz: Programmable internal frequency (PLL x1, x2, x3, x4 and free running mode(s)).
- **Adjustable internal frequency according to available power or required performance**
  - Increased internal frequency for maximum performance
  - Internal frequency is automatically adjusted to guarantee a given limited power consumption
- Two 16-bit autoreload timer
- Power saving sleep mode
- **Ext. Clock freq. 1 up to 7.5 MHz**
- **UART for handling serial interface** in accordance with ISO/IEC 7816 part 3 **supporting transmission protocols T=1 and T=0**
- Supply voltage range:1.8 V, 3.0 V, 5.0 V
- Support of current consumption limits by GSM / UICC applications
  < 10 mA @ 5.5 V
  < 6 mA @ 3.3 V
  < 4 mA @ 1.98 V
- Operating Temperature range: -25 to +85°C
- Storing temperature range: -40° to +125°C
- ESD protection larger than 6 kV (HBM)

E²PROM Technology

- Write cycle time 0.7ms
- Erase cycle time 0.7 ms
- Typical programming time (erase & write) incl. firmware 2 ms
- Fast personalization mode < 0.9 ms per page
- Enhanced Error Correction Unit controlled by OS
- Reading and programming byte by byte
- Flexible page mode for 1 to 64 bytes write/erase operation
- 32 bytes security area (OTP)
- Minimum of 500.000 write/erase cycles @ 25°C per page. Maximum of 16.500.000 write/erase cycles per sector
- Typical data retention 10 years @ 25°C

Memory Management and Protection Unit

- Addressable memory of up to 16 Mbyte
- Separates OS (system mode) and application (user mode)
- System routines called by interrupts
- OS can restrict access to peripherals in application mode
- Variable application orientated segments defined and controlled by OS
- Code execution from XRAM possible
- Enhanced multi-application support by 16 descriptors for system / application mode.

Security Features

- Enhanced sensor concept:
  - Low and high voltage sensors
  - Frequency sensors and filters
  - Light Sensor
  - Glitch Sensors
  - Temperature Sensor
  - Life Test Function for Sensors (UMSLC)
- Bus confusion
- Security reset detection
- Current control oscillator (ICO)

Memory Securtiy

- Sparkling SFR encryption for DDES and ACE, CRC module and RNG
- 32 bytes security PROM, hardware protected for batch-, wafer-, die-individual security data. Unique chip identification number for each chip
- Additional memory for customer-defined security FabKey on request
- MED – memory encryption/decryption device for XRAM, ROM and EEPROM
- Security optimized layout and layout scrambling
- Fast IRAM erase
- Enhanced Error correction unit (ECU)

Testmode

- Irreversible Lock - Out of test-mode

Anti Snooping

- Automatic randomization smoothing of power profile
- Effective HW-countermeasures against SEMA/DEMA, SPA/DPA, DFA and Timing-Attacks
- Non standard dedicated Smart Card CPU – Core
- Active Shield with automatic and user controlled attack detection
- Hardware countermeasures controlled by True Random Number Generator

Targeted Certifications

- CC EAL5+
- VISA level 3
- MULTOS
- CAST

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
- ETSI TS 102 221

Document References

- Confidential Data Book SLE66CxxxPE
- 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 ROM Monitor RM66PE
- Short Product Information Emulator ET66PE Hitex or ET66PE KSC
- Short Product Information Smart Mask Package

Performance Advance Crypto Engine (ACE)

Operation		Run time (ms)		
		5 MHz	15 MHz	33 MHz
RSA 1024	Sign (w CRT)	568 ms	189 ms	86 ms
	Verify (F_4)	20 ms	7 ms	3 ms
RSA 1536	Sign (w CRT)	1129 ms	376 ms	171 ms
	Verify (F_4)	581 ms	194 ms	88 ms
RSA 2048	Sign (w CRT)	1881 ms	627 ms	285 ms
	Verify (F_4)	812 ms	271 ms	123 ms

(typical values including software overhead for security protection, based on internal test results)

Performance DDES-Accelerator

Operation	Data Block Length	Encryption Time for an 8Byte Block incl. Data Transfer		
		5 MHz	15 MHz	33 MHz*
112-bit Triple DES Encryption	64 bit	35 µs	12 µs	5 µs

(typical values, based on internal test results)

Ordering Information

Type	Package[1]	Voltage Range	Temperature Range	Frequency Range (int. clock frequency)	Frequency Range (ext. clock frequency)
SLE 66CX480P**E** C	Die (sawn, unsawn)	1.8 V; 3.0 V; 5.0 V or 3.0 V; 5.0 V	- 25°C to + 70°C or - 25°C to + 85°C	Up to 33 MHz	1 MHz - 5 MHz or 1 MHz - 7.5 MHz
SLE 66CX480P**E** M5	M5.1				
SLE 66CX480P**E MFC5.6**	MFC5.6				
SLE 66CX480P**E MFC5.8**	MFC5.8				
SLE 66CX480P**E DSO-8**	DSO-8				

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

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

Pin Configuration

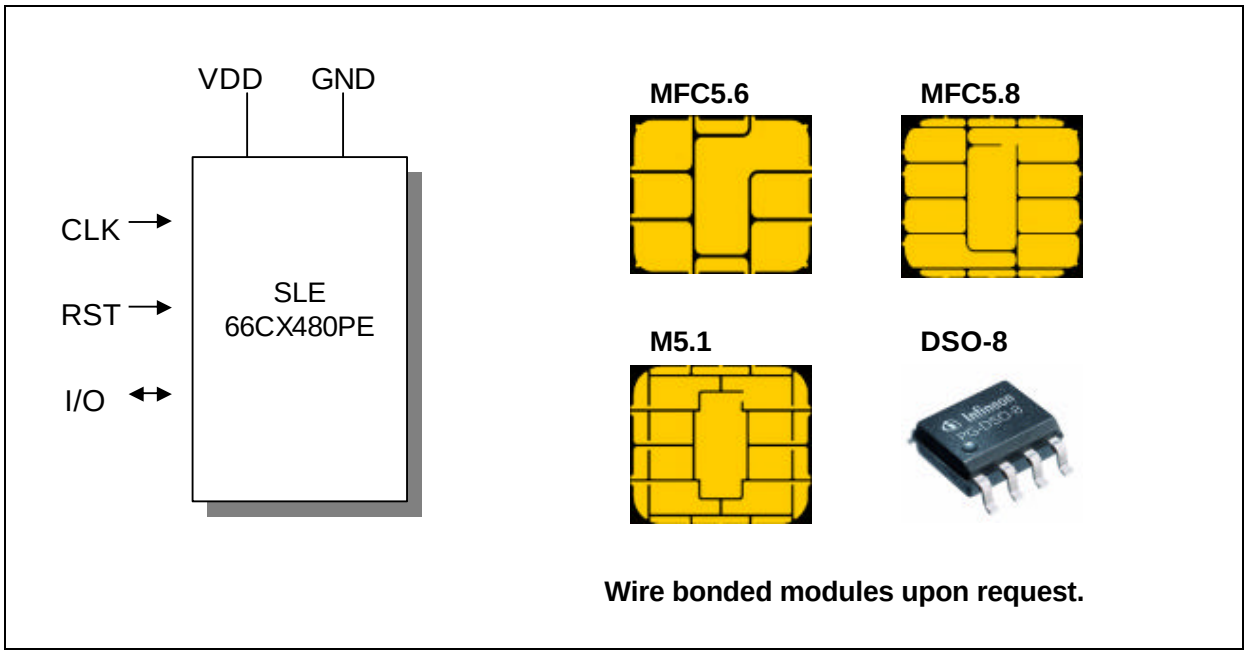

Figure 1: Pin Configuration

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

The SLE66CX480PE is another member of the improved 66PE-series of Infineon Technologies. This high performance security crypto controller is manufactured in advanced 0.22 µm CMOS technology. It is downward compatible to existing 66P controller derivatives. The well known ECO2000 8/16 bit 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 compared to existing 66P derivatives.

Performance

The internal clock frequency can be adjusted to a level up to 33 MHz either as a multiple of 1,2,3,4 to the external frequency or independent of the clock rate of the terminal with the help of the internal clock. It is adjustable according to either available power requirements or required performance:

- Increased internal clock frequency for maximum performance, e.g. for high performance with max. frequency in payment applications or crypto operations.
- Automatically adjusted frequency for a max. given power consumption, e.g. by GSM or UMTS requirements.

Memory

The SLE66CX480PE offers 244 Kbytes of User-ROM, 256 byte internal RAM, 6144 byte XRAM and 48 Kbytes MicroSlim-EEPROM, to fulfill the increased requirements of GSM and UMTS applications. The large ROM size allows to place applications in the ROM-mask and to keep the E²PROM free for customer data. In addition it saves mask development costs, as one mask may be used for different customer projects. 48 Kbyte of EEPROM thus allows to include SIM Application Toolkit, Wireless Application Protocol (WAP), WML-Browser and JavaCard API implementations into the NVM.

Memory (cont'd)

The enhanced Memory Management and Protection Unit allows a secure separation of the operating system and different applications. It allows to separate the memories in application orientated segments, which can be controlled by the OS. Furthermore, the MMU makes a secure downloading of applications possible even after personalization of a card. These new features suit the requirements of the next generation of multi-application operating systems.

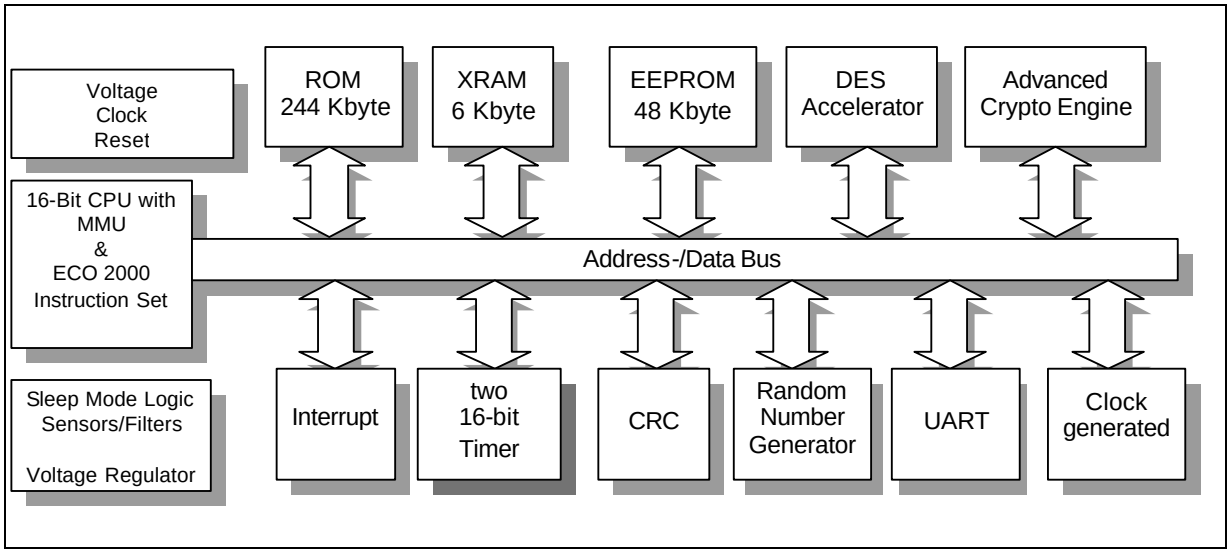

Figure 2: Block Diagram SLE 66CX480PE

The new platform is designed to address up to 16 Mbyte. However this feature is only available upon request and will clearly require a change in the existing tool environment.

In addition, new instructions have been implemented in the design for an efficient direct access of physical memory >64Kbyte up to 16 Mbyte.

Security features

Since the very beginning, security is an integrated part of Infineons product development, as proved by various certificates (ITSEC, CC, Proton, VISA, ZKA, Mondex). The so called **"integral security concept"** for the 66PE series ensures:

- A secret storage of any confidential code, data and keys
- Protection against side channel attacks such as: Simple Power Analysis (SPA) , Differential Power Analysis (DPA),
- Protection against Differential Fault Analysis (DFA), Electromagnetic Emanation Attack (EMA) and other possible HW or SW attacks

Peripherals

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 (ACE) 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 either in HW or supported by software of e.g. RSA operations and EC (Elliptic Curves) algorithms for key lengths up to 2048-bit.

For all of its crypto controller using the ACE, Infineon offers a tailor made RSA 2048-bit library. This library is a powerful multifunctional crypto library for the SLE 66CXxxPE family. It provides arithmetic functions for easy programming the Advanced Crypto Engine (ACE). In addition it provides a full implementation of RSA Sign, Verify and Key generation including powerful SPA/DPA and DFA counter measures. It supports RSA up to 2048 bit key length. These RSA functionality is included in Common Criteria EAL5+ certification of SLE 66CXxxPE controllers.

The HW-DES module supports symmetric crypto algorithms according to the Data Encryption Standard in the Electronic Code Book Mode.

The random number generator (RNG) is able to supply the CPU with true random numbers on all conditions. It is compliant with AIS-31.

The advanced sensor concept includes various sensors for any kind of attack scenarios and even more important a "Life Test " for sensors.

As an important feature, the chip provides an on-chip security, which fulfills the strong security requirements of a Common Criteria evaluation at an EAL5+ level.

In conclusion, the SLE 66CX480PE fulfills all the requirements of today's chip card applications, and is especially designed for DDA payment, GSM, PayTV and ID-applications incl. digital signatures. In addition it offers a powerful platform for multi application cards based on Multos or Java and supports the migration to enhanced GSM (incl. WAP), GPRS and UMTS value added services.

The SLE66CX480PE integrates outstanding memory sizes, in combination with enhanced performance and optimized power consumption on a minimized die size.

Glossary

CLK	Clock
CRC	Cyclic Redundancy Check
CPU	Central Processing Unit
CMOS	Complementary Metal-Oxide Semiconductor (technology used to manufacture most of today's chips)
E²PROM	Electrically Erasable Programmable Read-Only Memory (equivalent to NVM)
ESD	Electrostatic Discharge, release of static electricity that can damage a chip
FIFO	First In, First Out
GND	Ground
I/O	Input/Output
MED	Memory Encryption Decryption unit
MMU	Memory Management Unit
NVM	Non Volatile Memory (equivalent to E²PROM)
OS	Operating System
OTP	One Time Programmable (equivalent to PROM)
PROM	Programmable Read-Only Memory (equivalent to OTP)
RAM	Random Access Memory
RMS	Resource Management System
RNG	Random Number Generator
ROM	Read-Only Memory
RST	Reset
SDK CC	Software Development Kit Chip Card
STS	Self Test Software
T=0, T=1	Communication Protocols defined in ISO 7816 standard
TRNG	True Random Number Generator
UART	Universal Asynchronous Receiver/Transmitter
Vcc	External Voltage (common-collector voltage)
PLL	Phase-Locked Loop
XRAM	eXternal Random Access Memory

Sales code name