Chip Card & Security

SLE 66CL81PE(M) Family

8/16-Bit High Security Contactless Controller
For Contactless Applications

ISO/IEC 14443 Type B & A Compliant Interfaces

with Linear Addressing Instruction Set For Large Memories
in 0.22 µm CMOS Technology

92-Kbyte User ROM, 2304-byte RAM,
8-Kbyte EEPROM

112-Bit Dual Key DES Accelerator
supporting DES, 3DES Algorithms

Short Product Information 12.2009

Preliminary SLE 66CL81PE(M) Family Short Product Information Ref.: SPI_SLE66CL81PE_091106.doc	
This document contains preliminary information on a new product under development. Details are subject to change without notice. **Revision History: Current Version: 2009-12-16**	
Previous Releases:	
Page	Subjects (changes since last revision)

Important: Further information is confidential and on request. Please contact:
Infineon Technologies AG in Munich, Germany,
Chip Card & Security
Email: security.chipcard.ics@infineon.com
www.infineon.com/security

Published by Infineon Technologies AG,
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 High Security Contactless Controller in 0.22 µm CMOS Technology for Contactless Operation with ISO/IEC14443 Type B & A Compliant Interfaces

with MMU and Linear Addressing Instruction Set For Large Memories and optional MIFARE™ compatible emulation
92-Kbyte User ROM, 2304-byte RAM, 8-Kbyte EEPROM
112-Bit Dual Key DES Accelerator supporting DES, 3DES algorithm

General Features

- Enhanced low power non-standard architecture 8051 CPU with extended addressing modes for contactless smart card applications
- Instruction set opcode compatible with standard 8051 processor with additional powerful instructions optimized for smart card application
- Execution time at least 6 times faster than standard 8051 processor at same external clock
- Additional enhanced instructions for direct physical memory access of >64-Kbyte
  - Typically saves up to 90 % code space and increases execution speed up to 80%
- 92-Kbyte User ROM for operating system and application (programs & data)
  - 256 bytes reserved ROM for Resource Management System (RMS) with Contactless optimized EEPROM write/erase routines
- 8-Kbyte Secure EEPROM in MicroSlim technology for application program and data
- MIFARE™ compatible emulation
  - 4-Kbyte reserved in User ROM
  - 2-Kbyte additional EEPROM protected by RMS Firewall
- 2048-byte XRAMand 256-byte internal RAM for fast data processing
- Enhanced Memory Management Unit with application and user defined segment
- EEPROM voltage generated on chip
- Certified True Random Number Generator with firmware test function supporting AIS-31 requirements
- Dual Key Triple DES (DDES) Accelerator
- CC EAL5+ Certification planned according to BSI–PP-0002
- CRC Module according to ISO/IEC 3309 supporting CCIT V.41 & HDLC X25 with configurable initial values
- 16 Interrupt Vectors Module with 3 priority levels to ensure real time operation
- Internal clock controlled by PLL: up to 30MHz asynchronous clock frequency (optional use)
- Adjustable internal frequency according to available power or required performance
  - Increased internal frequency for maximum performance
  - Internal frequency adjusted to guarantee a given limited power consumption
- Two 16-bit Auto-reload Timers with interrupt capability for protocols, security checks & watch dog implementations
- Power saving sleep mode
- Temperature range:
  contact-less: -25°C to +70°C

MIFARE™ is a trademark of NXP B.V.

Contactless Interface

- Interface according to ISO/IEC 14443 for both Type B and Type A
- Carrier frequency 13.56 MHz
- Data rate in both directions
  up to 848 Kbit/s in type B operation
  up to 848 Kbit/s in type A operation
- Anticollision & Transmission Protocol supported by open source application notes for both Type B & A
- Flexible Internal CPU clock frequency: fully configurable from 1.7 MHz up to 30 MHz
- 256 bytes buffer for contactless data exchange (FiFo circular architecture)

Memory Management and Protection Unit

- Addressable memory up to 16 Mbytes
- Separates OS (system mode) and Application (application mode) by usage of descriptors
- Enhanced multi-application support by 16 descriptors
- System routines called by interrupts
- Access Restrictions to peripherals in application mode controlled by OS
- Code execution from XRAM possible
- Secure start of the operating system ensured by certified Self Test Software (STS)
- Certified EEPROM programming routines (RMS)
- Enhanced Error Correction Unit (ECU)
- Certified True Random Number Generator including firmware test function supporting AIS-31 requirements.
- High Speed SPA/DPA resistant Dual Key DES (DDES) Accelerator

MIFARE™ compatible interface

- **Optionally 1-Kbyte emulation**
- Operation controlled by RMS functions: same functionality and command set as given by the MIFARE™ technology
- Support of multiple MIFARE™ compliant interfaces on one controller
- Unique Identification number
- Personalisation also possible in Contact based mode secured by RMS functions

E²PROM Technology

- Byte wise EEPROM programming and read accesses
- Flexible page mode for 1 to 64 bytes write/erase operation
- 32 bytes security area including:
  - 16 bytes chip unique identification number
  - 16 bytes PROM area (OTP like)
- Fast personalisation mode =1.0 ms
- Typical Page Programming time of 2.2ms
- Enhanced ECC Module controlled by Operating System
- Platform prepared for flash-like erasing of up to 2-Kbyte EEPROM-segments
- **Minimum of 500.000 Write/erase cycles @25°C** per page
- Data retention for a minimum of 25 years @25°C
- EEPROM programming voltage generated on chip

Security Features

Operation state mechanism

The chip goes in a secure reset state on any following sensor alarm:

- Low and high voltage sensors
- Internal voltage sensor
- Frequency sensors and filters
- Light sensor
- Glitch sensors
- Temperature sensor
- Life Test function for sensors
- Internal power-on reset sensor
- Active Shield with automatic and user controlled attack detection

Secure chip and firmware design

- Sparkling SFR encryption for DDES, ACE, RNG and CRC modules
- Security scrambled, dual rail pre-charge logic design & optimized chip layout against physical chip manipulation
- Bus Confusion
- Immediate internal RAM erase upon security reset detection
- Security Reset
- ROM code not visible due to implantation
- Mask dependant ROM code encrypted during production
- Chip unique encryption of the XRAM and EEPROM
- Flexible encryption of part or whole EEPROM by additional user-defined key
- Memory encryption/decryption module (MED) for XRAM, ROM and EEPROM against reverse engineering and power attacks
- 16 byte Unique Chip Identification number for anti-clone countermeasure & secure tracking
- 16 bytes security PROM hardware protected (OTP like)

Application Support

- HW-& SW-Tools (Emulator, ROM Monitor,

Anti Snooping

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

Targeted Evaluation

- CC EAL5+
- Visa Level 3
- CAST
- EMVCo

Supported Standards

- EMV 2000
- MasterCard PayPass® M/Stripe and M/Chip
- Visa Wave® and MSD
- ISO/IEC 14443
- ISO/IEC 3309
- CCIT v.41
- HDLC X25

Simulator, Evaluation Kit Proximity (Contactless Reader package), SmartMask™ package, Simulated Reader Software, etc.)

- Open Source Application Notes Tutorial (e.g.: T=0, T=1, DES and 3DES, Crypto Library, Anticollision and Contactless Transmission Protocols for both Type B and A, Card Coil Design Guide, Card Coil Antenna Reference Design List, etc.)
- Certified CC EAL5+ Crypto Library
- Worldwide Application Engineer Team and customer dedicated Field Application Engineers
- Dedicated Team for Contactless Design-in support and Analysis
- Regular Customer trainings on Cryptography, Contactless and Dual interface controllers including ISO/IEC 14443 related topics
- On-site trainings available on request

Document References

- Confidential Data Book SLE 66CL(X)xxxPE(M)
- Confidential Instruction Set SLE 66CxxxPE(M)
- Confidential Quick Reference SLE 66CxxxPE(M)
- Chip Qualification report
- Chip delivery specification for wafer with chip-layout (die size, orientation, ...)
- Module specification containing description of package, etc.
- Module Qualification report

Development Tools Overview

- Straight forward migration of existing tool chain for 66P towards 66PE family by firmware update
- Software Development Kit SDK CC
- ROM Monitor RM66P/PE-II with stand alone functionality for ROM mask qualification in the end user system
- Emulator ET66P/PE Hitex or ET66P/PE KSC
- Smart Mask™ Package for chip evaluation
- Smart Mask™ Contactless only modules MCC8(supplied by Infineon) supporting ISO/IEC 14443 Type B & Afor implantation process testing and production setup
- Evaluation Kit Proximity (Contactless reader package)
- Reader Optimization Kit

Cryptographic Timing Performances

Operation	Data Block Length	Encryption Time for an 8-byte Block including Data Transfer		
		5 MHz	15 MHz	30MHz
High Speed and Secure 56-bit **Single DES Encryption (incl. key loading)**	64 bit	37 µs	12 µs	6 µs
High Speed and Secure 56-bit Single DES Encryption	64 bit	23 µs	8 µs	4 µs
High Speed and Secure 112-bit **Triple DES Encryption (incl. key loading)**	64 bit	60 µs	20 µs	10 µs
High Speed and Secure 112-bit Triple DES Encryption	64 bit	35 µs	12 µs	6 µs

Table 1 Performance DDES Accelerator[1]

Ordering Information

Type	Package	Temperature Range	Frequency Range[2] (external clock CL)	Frequency Range (internal clock)
SLE 66CL81PE(M) – MCC8	MCC8[3]	– 25°C to + 85°C	13.56MHz	Up to 30MHz
SLE 66CL81PE(M) – C	Chip			

Table 2 Package Product Information[4]

[1] Preliminary values based on internal test results
[2] External Contactless clock range according to ISO/IEC14443
[3] Pure Contactless Module (MCC8): for standard thickness inlays (330µm)
[4] Ordering Codes are available on request

Pin Description and Pad Configuration

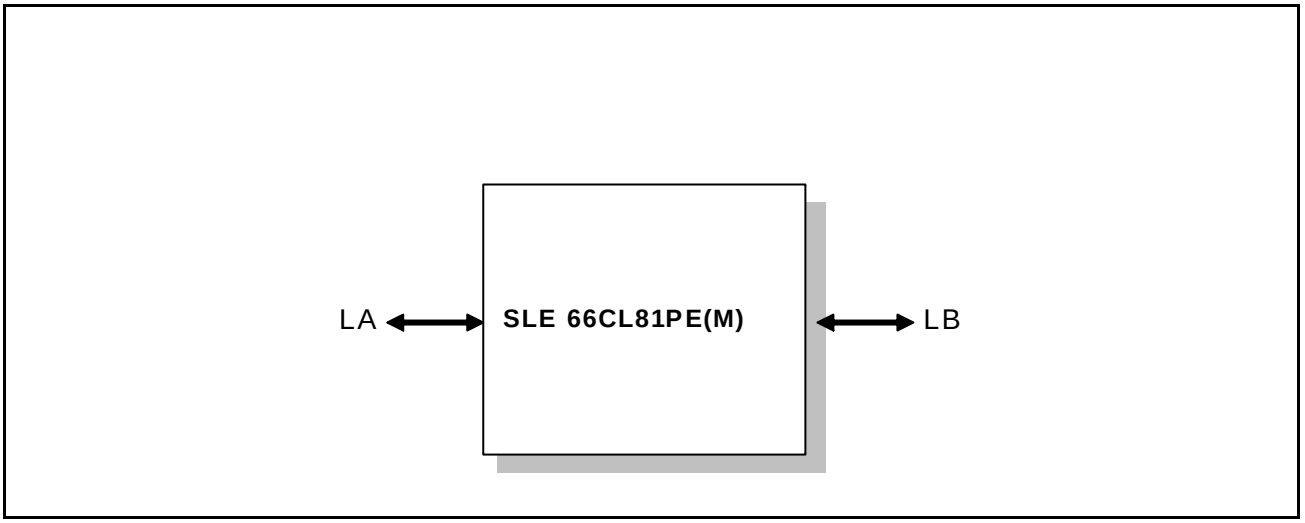

Figure 1 Pad Configuration (die)

Symbol	Function
LA	Coil connection pin LA
LB	Coil connection pin LB

Table 3 Pin Definitions and Functions

Block Diagram Description

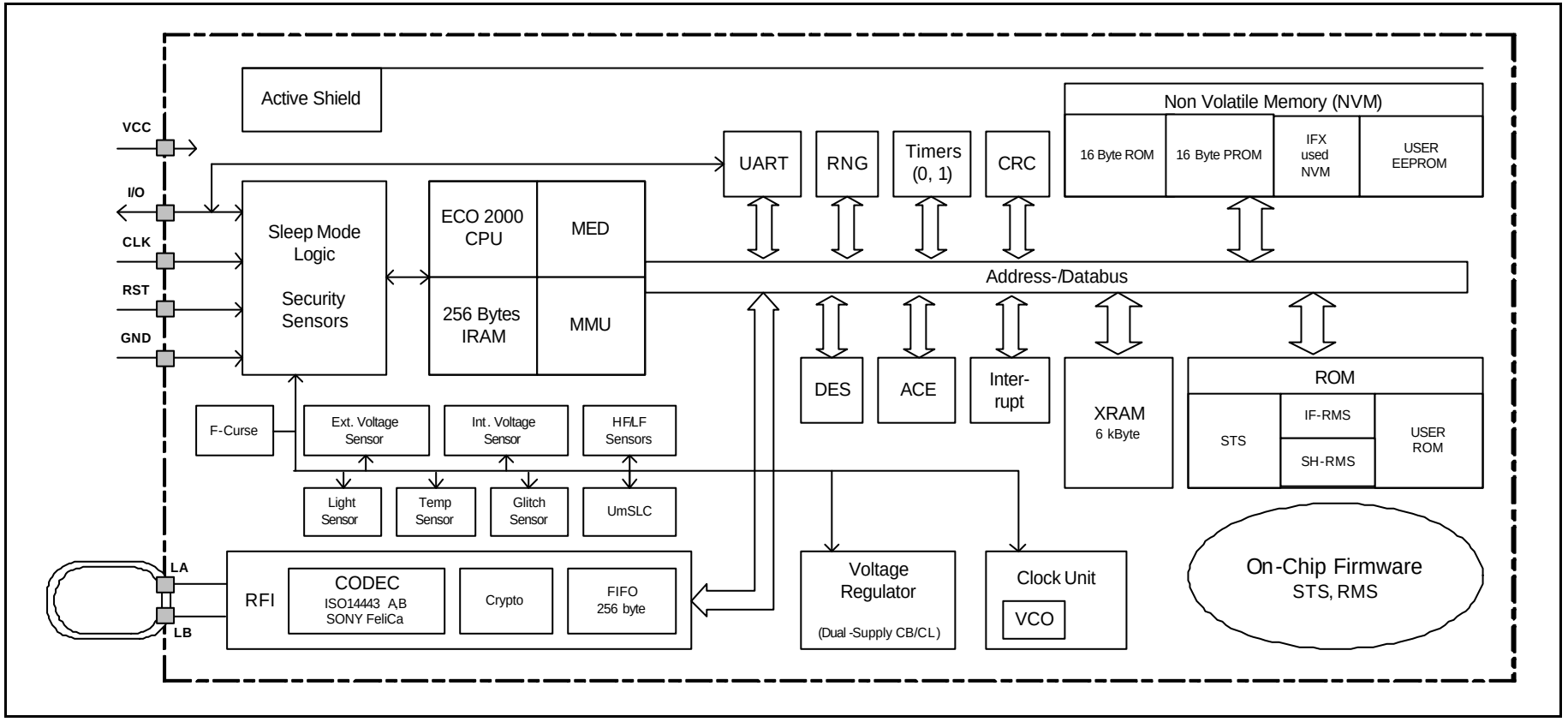

Figure 3 Block Diagram of SLE 66CL81PE(M)

General Description

The **contactless security controllers SLE 66CL81PE(M)** belong to the family of the Infineon Technologies SLE 66CxxxPE high-end security controller family in 0.22 µm CMOS technology which **are designed for contactless security systems** that requires continuous ongoing improvements **with the highest degree of protection against fraudulent attacks**.
SLE 66CL81PE(M) is targeting pure contactless smart card applications such as ID cards, banking, security access and transport.
SLE 66CL81PE(M) offers 92 Kbytes of User-ROM, 256 bytes internal RAM, 2 Kbytes XRAM and 8 Kbytes EEPROM, which can be used as data and as program memory. The non-volatile memory consists of high reliability cells to guarantee data integrity. This is especially important when the EEPROM is used as program memory.
It features **ISO/IEC 14443 Type B contactless interfaces** on a single chip **and Type A** They also support symmetric algorithms, such like DES and 3DES, independently of the communication mode.
The CPU provides the high efficiency of the 8051 instruction set extended by additional powerful instructions with enhanced performance, memory sizes and security features tailored forcontactless smart card applications. Using the embedded PLL, the internal clock is adjustable up to 30 MHz independent from the carrier frequency of the magnetic field supplied by the contactless terminal.
The Memory Management Unit allows a secure separation of the operating system and the applications. Using the system/application mode, it allows to securely downloading applications in the field after card personalisation. Using the MMU transparent mode allows keeping the memory mapping for code compatibility to previous 66P Infineon security controller family member. These new features suit the requirements of the new generation of operating systems.
To minimize the overall power consumption, the smart card controller can be set into sleep mode supporting clock stop mode.
Timers ease the implementation of advanced communication protocols such as T=CL (according to ISO/IEC 14443-4) and all other time critical processes for contactless communications. Both Timers features auto-reload mechanisms as well as their own dedicated interrupt vectors. Additional interrupts capability of the RF interface module allows real time operation of the pure contactless smart card with the contactless terminals.

SLE 66CL81PE(M) is able to communicate with any Proximity Card Device (PCD) defined in ISO/IEC 14443 such as the Infineon Evaluation Kit Proximity. The power supply and data are received by an antenna, which consists of a coil with a few turns directly connected to the IC. DES acceleration by a factor of more than 500 compared to software solutions in combination with the **high data transfer rate up to 848 Kbit/s keep the transaction times short. For more independence and flexibility, the controller offers the two modulation type B and type A according ISO/IEC 14443.**

The Anticollision and Contactless Transmission Protocol are supported by open source application notes for both Type B and A in order to **offer a maximum flexibility to the Operating System. Both Contactless Communication protocol may be implemented in the Operating System while the final selection of the Type B or A is based upon the personalisation data of the contactless smart card**. The communication type can also be changed during runtime in the field. Thus, **SLE 66CL81PE(M) ensures a simplified handling of the ROM mask, high reactivity by a tailored personalisation during production** of the contactless smart card in **order to answer to the increasing market demand and applications**.

SLE 66CL81PE(M) features a **new Resource Management System** (RMS_E) which **optimizes Contactless EEPROM write/erase routines**. EEPROM programming is enhanced over the entire communication distance compared to the standard RMS. Thus, the reduction of programming times and power consumption is ensured independently of the use of the contact or the contactless interface.
The **CRC module** allows the easy generation of checksums according to ISO/IEC 3309 (16-Bit-CRC), thus it **supports the two different CRC calculation required for ISO/IEC 14443 Type B and Type A**. It **additionally features an configurable initial value to avoid checksum computation re-starting from zero** in the case interrupts requiring use of the CRC module are triggered. Therefore, data as well as program located in the EEPROM can be extra-secured by a CRC checksum enabling the Operating System to detect errors while downloading new application in the field.
To minimize the overall power consumption, the pure contactless smart card controller can be set into sleep mode.
The certified random number generator (RNG) is able to supply the CPU with true random numbers on all conditions. It allows creating session key used for authentication in open networks and enable secure downloading of new applications.

The **DDES module** supports symmetrical crypto algorithms according to the Data Encryption Standard in the Electronic Code Book Mode. It features two internal registers for storage of the two keys required for a Triple DES computation. Together with the fast contactless interface, it **offers high security and high speed for contactless smart card applications**.

As an important feature, **SLE 66CL81PE(M) provides a new and enhanced level of on-chip security, which fulfils the strong security requirements of a Common Criteria evaluation at an EAL5+ High level**. Each security measure is designed to act as an integral part of the complete system in order to strengthen the system as a whole.

Thus, porting an **existing Operating System to SLE 66CL81PE(M) requires only very limited changes** as it is typically reduced to add the Contactless Library and the Contactless Optimized Resource Management System (RMS_E) to the existing Operating System.
SLE 66CL81PE(M) integrates outstanding memory sizes, additional peripherals in combination with enhanced performance and optimized power consumption on a minimized die size.

In conclusion, SLE 66CL81PE(M) fulfils the requirements of contactless smart card applications such like ID cards, banking, security access and transport. The family concept offers to select the right product for a given application in terms of available memory and price.

Glossary

AES	Advanced Encryption Standard
AIS-31	Functionality classes and evaluation methodology guidelines for physical random number generators defined by the German Institute for the Security of the Information Technology.
Caches	Cache memories are Random Access Memories that the CPU can access more quickly than it can access regular RAM.
CLK	Clock
CPU	Central Processing Unit
CMOS	Complementary Metal-Oxide Semiconductor, the technology used to manufacture most of today's microchips.
CRT	Chinese Remainder Theorem, computing technique
DES, 3DES	Data Encryption Standard
DSA	Digital Signature Algorithm
EAL 5+	Common Criteria Certification level
EC	Elliptic Curves
EEPROM	Electrically Erasable Programmable Read-Only Memory
ESD	Electrostatic Discharge, release of static electricity that can damage a chip
Exponent	Component of RSA key
F_4	Fermat Number F_4, computing term.
GF(2^m)	Galois Field: finite field of 2^m elements represented by polynomials with degree < m
GF(p)	Galois Field, set of whole numbers less than prime number *p*
I/O	Input/Output
Modulus	Component of RSA key
RAM	Random Access Memory
RISC	Reduced Instruction Set Computer
RNG, TRNG	Random Number Generator, True Random Number Generator
ROM	Read-Only Memory
RSA	Rivest, Shamir and Adleman, inventors of the RSA cryptosystem
SHA-1	Secure Hash Algorithm revision 1
STS	Self Test Software
T=0, T=1	Communication Protocols defined in ISO 7816 standard
UART	Universal Asynchronous Receiver/Transmitter

Sales code name