Security & Chip Card ICs

SLE 66CLX641P

16-Bit High Security Contactless Controller
ISO/IEC 14443 Type A & B Compliant Interfaces
For Contactless Operation

with Memory Management and Protection Unit
in 0.22 µm CMOS Technology
136-Kbyte ROM, 5-Kbyte RAM, 64-Kbyte EEPROM
1100-Bit Advanced Crypto Engine
supporting RSA and Elliptic Curve GF(p)
112-Bit / 192-Bit DDES-EC2 Accelerator
supporting DES, 3DES and Elliptic Curve GF(2^n)

Short Product Information April 2004

SLE 66CLX641P Short Product Information	Ref.: SPI_SLE66CLX641P_0404.doc
This document contains preliminary information on a new product under development. Details are subject to change without notice.	
Revision History: Current Version 2004-04-27	
Previous Releases: 2004-04-01	
Page	

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

Published by Infineon Technologies AG, SMS Security Applications Group
St.-Martin-Strasse 53, D-81541 München

To our valued customers

We constantly strive to improve the quality of all our products and documentation. We have spent an exceptional amount of time to ensure that this document is correct. However, we realise that we may have missed a few things. If you find any information that is missing or appears in error, please use the contact section above to inform us. We appreciate your assistance in making this a better document.

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 High Security Contactless Controller
ISO/IEC 14443 Type A &B Compliant Interfaces
For Contactless Operation with MMU in 0.22 µm CMOS Technology
136-Kbyte ROM, 5-Kbyte RAM, 64-Kbyte EEPROM
1100-Bit Advanced Crypto Engine supporting RSA and Elliptic Curve GF(p) and
112-Bit / 192-Bit DDES-EC2 Accelerator
supporting DES, 3DES and Elliptic Curve GF(2n)

Features

- Enhanced **low power 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
- Enhanced architecture with **execution time 6 times faster (18 times using PLLmax)** than standard 8051 processor at same external clock
- **134 Kbytes User ROM** for operating system and application (programs & data)
- **2 Kbytes reserved ROM for** Resource Management System **(RMS_E)** with **Contactless Optimized EEPROM write/erase routines**
- **64 Kbytes Secure EEPROM in SuperSlim technology for application program and data**
- **4k bytes XRAM, 700 bytes Crypto-RAM and 256 bytes internal RAM for fast data processing**
- **Memory Management Unit**
- **Certified True Random Number Generator**
- **Dual Key Triple DES (DDES) & GF (2^n) Elliptic Curve (EC2) Accelerator**
- **Advanced Crypto Engine for Elliptic Curve GF(p) and up to 2048 bits RSA computation**
- CRC Module according to ISO/IEC 3309 supporting CCIT v.41 & HDLC X25
- 8 Interrupt Vectors Module with 3 priority levels to ensure real time operation
- **PLL: to speed up the internal CPU clock frequency up to 15MHz** (optional use)
- Two 16-bit Timer with interrupt capability for protocols, security checks & watch dog implementations
- Power saving sleep mode
- Temperature range:
  contact-less: -25°C to +70°C

Full operation of Contactless interface controlled by Operating System enhances Security Level

Contactless Interface

- **Interface according to ISO/IEC 14443 for both Type A and Type B**
- Carrier frequency 13.56 MHz
- Data rate
  106 Kbit/s in type A operation
  up to 848 Kbit/s in type B operation
- **Anticollision & Transmission Protocol supported by open source application notes for both Type A & B**
- **Flexible Internal CPU clock frequency: fully configurable from 1.7MHz up to 15 MHz**
- **256 bytes buffer for contactless data exchange (FiFo circular architecture)**
- **Parallel operation of CPU, Peripherals like DES, CRC and Contactless Interface possible for High Demanding Contactless Applications**

EEPROM (SuperSlim Technology)

- Byte wise EEPROM programming and read accesses
- Versatile & Flexible page mode for 1 to 256 bytes write/erase operation
- 32 bytes security area including:
  - 16 bytes chip unique identification number
  - 16 bytes PROM area (OTP like)
- Fast personalisation mode 1.5 ms
- Typical Page Erase time < 2.5ms
- Typical Page Writing time < 1.8 ms
- **Minimum of 100.000 Write/erase cycles**[1)]
- Data retention for a minimum of 10 years[1)]
- EEPROM programming voltage generated on chip

Memory Management and Protection Unit

- Addressable memory up to 1 Mbytes
- Separates OS (system mode) and Application (application mode)
- System routines called by traps
- Access Restrictions to peripherals in application mode controlled by OS
- Code execution from XRAM possible

Security Features

Operation state monitoring mechanism

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

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

Secure chip and firmware design

- Security scrambled & optimized chip layout against physical chip manipulation
- Memory encryption/decryption module (MED) for XRAM, ROM and EEPROM against reverse engineering and power attacks
- 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
- 16 byte Unique chip identification number for anti-clone countermeasure & tracking
- 16 bytes security PROM hardware protected (OTP like)
- Secure start of the operating system ensured by certified Self Test Software (STS)
- Certified EEPROM programming routines (RMS_E)
- True Random Number Generator with Firmware test function
- High Speed SPA/DPA resistant Triple DES (DDES) Accelerator and Advanced Crypto Engine

Anti Snooping

- HW-countermeasures against SPA/DPA-, Timing- and DFA-attacks (differential fault analysis)

Supported Standards

- EMV 2000
- ISO/IEC 14443
- ISO/IEC 3309
- CCIT v.41
- HDLC X25

[1)] Values are temperature dependant

Application Support

- HW-& SW-Tools (Emulator, ROM Monitor, Card Emulator, Simulator, Evaluation Kit Proximity (Contactless Reader package), SmartMask™ package, Simulated Reader Software, etc.)
- Open Source Application Notes Tutorial (e.g.: DES and 3DES, Crypto Library, Anticollision and Contactless Transmission Protocols for both Type A and B, 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
- 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 66CxxP
- Confidential Instruction Set SLE 66CxxP
- Confidential Quick Reference SLE 66CxxP
- 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

- Software Development Kit SDK CC
- Card Emulator CE66P Dual Interface
- ROM Monitor RM66P-II with stand alone functionality for ROM mask qualification in the end user system
- Emulator ET66P Hitex or ET66P KSC
- Smart Mask™ Package for chip evaluation
- Smart Mask™ Pure Contactless modules (supplied by Infineon) supporting both ISO/IEC 14443 Type A & B for implantation process testing and production setup
- Evaluation Kit Proximity (Contactless reader package)

Timing performances are independent of the Type A or Type B contactless interface.

Table 1 Performance Advanced Crypto Engine

Operation	Modulus	Exponent	Calculation Time at 5 MHz	Calculation Time at 15 MHz
Modular Exponentiation	160 bit	160 bit	20 ms	7 ms
Modular Exponentiation	256 bit	256 bit	35 ms	12 ms
Modular Exponentiation	512 bit	512 bit	110 ms	37 ms
Modular Exponentiation RSA Encrypt / RSA Signature Verify	1024 bit	16 bit	20 ms	7 ms
Modular Exponentiation RSA Decrypt / RSA Signature Generate	1024 bit	1024 bit	820 ms	273 ms
Modular Exponentiation using CRT RSA Decrypt / RSA Signature Generate	eq.1024 bit	eq.1024 bit	250 ms	83 ms
DSA Signature Generate	512 bit	160 bit	145 ms	48 ms
DSA Signature Verify	512 bit	160 bit	130 ms	43 ms
DSA Signature Generate	1024 bit	160 bit	290 ms	97 ms
DSA Signature Verify	1024 bit	160 bit	360 ms	120 ms
Elliptic Curves EC-GDSA Sign. Generate	160 bit	160 bit	260 ms	87 ms
Elliptic Curves EC-GDSA Sign. Verify.	160 bit	160 bit	550 ms	183 ms

Features (cont'd)

Table 2 Performance DDES-EC2 Accelerator

Operation	Data Block Length	Encryption Time for an 8-byte Block including Data Transfer	
		5 MHz	**15 MHz**
High Speed and Secure 56-bit **Single DES Encryption (incl. key loading)**	64 bit	37 µs	12 µs
High Speed and Secure 56-bit Single DES Encryption	64 bit	23 µs	8 µs
High Speed and Secure 112-bit **Triple DES Encryption (incl. key loading)**	64 bit	60 µs	20 µs
High Speed and Secure 112-bit Triple DES Encryption	64 bit	35 µs	12 µs
	Operand Length	**Calculation Time**	
		5 MHz	**15 MHz**
Elliptic Curves GF(2^n) EC-DSA Signature Generate	192 bit	285 ms	95 ms
Elliptic Curves GF(2^n) EC-DSA Signature Verify	192 bit	540 ms	180 ms

Table 3 Ordering Information[1]

Type	Temperature Range	Frequency Range (external clock)
SLE 66CLX641P	– 25°C to + 70°C	13.56 MHz

[1] Ordering Code is available on request

Pin Description

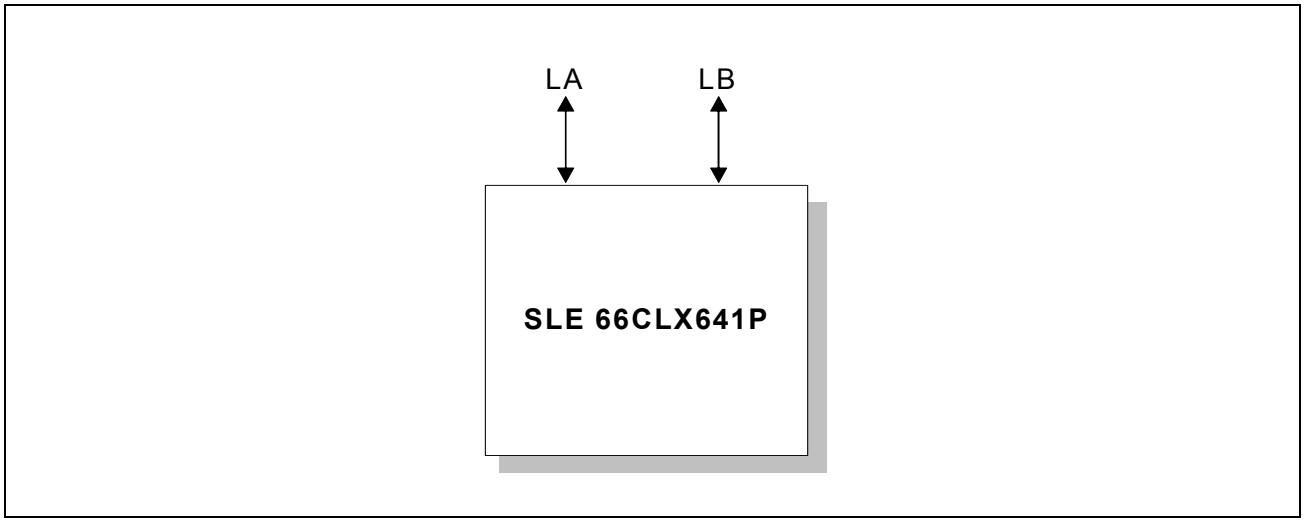

Figure 1 Pad Configuration (die)

Table 4 Pin Definitions and Functions

Card Contact	Symbol	Function
	LA	Coil connection pin LA
	LB	Coil connection pin LB

General Description

The **contactless only security controller SLE 66CLX641P** is a member of the Infineon Technologies SLE 66CxxxP high-end security controller family in 0.22 µm CMOS technology which **is designed for security systems** that requires continuous ongoing improvements **with the highest degree of protection against fraudulent attacks**.

SLE 66CLX641P is targeting contactless applications such like electronic passport, electronic visas, national ID cards, banking, security access, digital signature and transport.

SLE 66CLX641P offers 134 Kbytes of User-ROM, 256 bytes internal RAM, 4 Kbytes XRAM, 700 bytes Crypto RAM and 64 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 **both ISO/IEC 14443 Type A and B contactless interfaces on a single chip**. It also supports symmetric and asymmetric public-key algorithm such like DES, 3DES, Elliptic Curves and RSA independently of the communication mode.

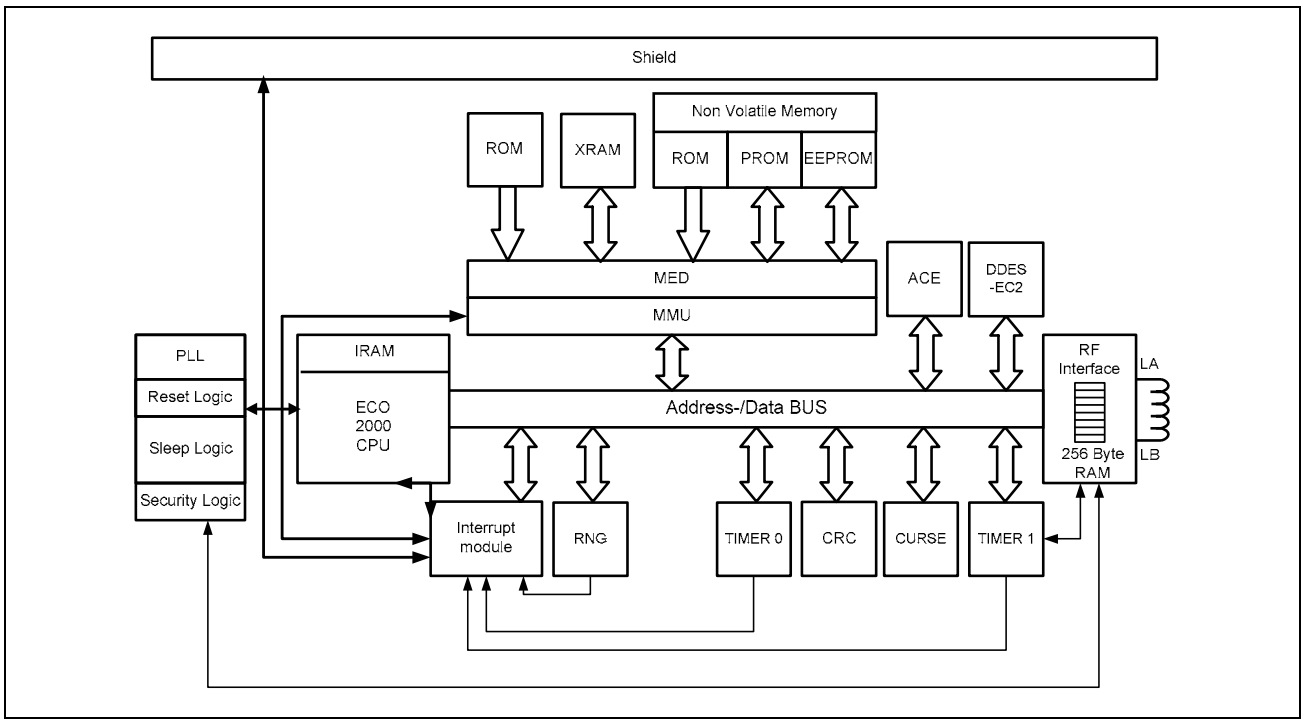

Figure 2: Block Diagram of SLE 66CLX641P

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 for contact and contactless smart card applications. Using the embedded PLL, the internal clock is adjustable up to 15 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 SLE 66CxxS family. These new features suit the requirements of the new generation of operating systems.

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 66CLX641P is able to communicate with any Proximity Card Device (PCD) defined in ISO/IEC 14443 such as the Infineon Evaluation Kit Proximity **over a typical coupling distance of 10 cm**. 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 A and type B according ISO/IEC 14443.**

The Anticollision and Contactless Transmission Protocol are supported by open source application notes for both Type A and B 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 A or B 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 66CLX641P 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 66CLX641P 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 A and Type B. Also, 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-EC2 accelerator consists of two modules.

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**.

The **EC2 module** accelerates the multiplication in GF (2^n) and therefore the operations for elliptic curve cryptography. It widens the field of application for SLE 66CLX641P since it **can be used as tamper-resistant security tool for secured and authentic communication in open networks** using contactless operation.

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 of e.g. RSA operations with key lengths up to 2048 bit and Elliptic Curve GF (p).

As an important feature, **SLE 66CLX641P provides a new and enhanced level of on-chip security, which fulfils the strong security requirements of a Common Criteria evaluation at an EAL5 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 66CLX641P requires only very limited changes** as it is typically reduced to remove the Contact-based communication library, add the Contactless Library and the Contactless Optimized Resource Management System (RMS_E) to the existing Operating System.

SLE 66CLX641P integrates outstanding memory sizes, additional peripherals in combination with enhanced performance and optimized power consumption on a minimized die size.

In conclusion, SLE 66CLX641P fulfils the requirements of contactless applications such electronic passport, electronic visas, national ID cards, banking, security access, digital signature and transport. In the case a dual interface security controller is required, SLE 66CLX640P offers an additional contact-based interface to the SLE 66CLX641P.