Security & Chip Card ICs

SLE 66CL160S

16-Bit High Security Dual Interface Controller
in 0.6 µm CMOS Technology
32-Kbyte ROM, 1280-byte RAM, 16-Kbyte EEPROM
112-Bit / 163-Bit DDES-EC2 Accelerator

Short Product Information

December 2001

SLE 66CL160S Short Product Information	Ref.: SPI_SLE66CL160S_1201.doc
Revision History: Current Version 2001-12-06	
Previous Releases: 06.00	
Page	
all	editorial changes

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, CC Applications Engineering 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 Dual Interface Controller in 0.6 µm CMOS Technology
32-Kbyte ROM, 1280-byte RAM, 16-Kbyte EEPROM
112-Bit / 163-Bit DDES-EC2 Accelerator

Features

- **16-bit microcomputer in 0.6 µm CMOS technology**
- Instruction set opcode compatible with standard 8051 processor
- Enhanced 16-bit arithmetic
- Additional powerful instructions optimized for chip card applications
- Dedicated, non-standard architecture with **execution time 6 times faster** than standard 8051 processor at same external clock
- **31.5 Kbytes User ROM** for application programs
- 512 bytes ROM for Resource Management System (RMS) with intelligent EEPROM write/erase routines
- **16 Kbytes EEPROM**
- **1 Kbytes XRAM, 256 bytes internal RAM**
- **True Random Number Generator**
- **Dual Key Triple DES (DDES) and GF (2^n) Elliptic Curve (EC2) Accelerator**
- CRC Module
- Interrupt Module
- Two 16-bit Autoreload Timer with 8-bit prescaler
- Power saving sleep mode
- Temperature range: -25°C to +70°C

EEPROM

- Reading, erasing and writing byte by byte
- Flexible page mode for 1 to 64 bytes write/erase operation
- 32 bytes security area
- Write time 3.6 ms, erase time 1.8 ms
- Programming time adaptable to clock frequency
- **Minimum of 500.000 write/erase cycles**[1)]
- Data retention for a minimum of 10 years[1)]
- EEPROM programming voltage generated on chip

Full operation either via Contact-based or Contactless interface controlled by Operating System

Contact-based Interface

- **Contact configuration and serial interface according to ISO/IEC 7816**
- Supply voltage range: 2.7 V to 5.5 V
- Current consumption < 10 mA @ 5 MHz and 5.5 V
- CPU clock frequency: 1 to 5 MHz (internal clock = external clock)
- I/O routines realized in software
- ESD protection larger than 4 kV (ISO pads)

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 for both types
- Anticollision and Transmission Protocol supported by software
- Internal CPU clock frequency: 1.13 MHz (f_C/12) to 3.39 MHz (f_C/4)
- 127 bytes buffer for data exchange (FiFo circular architecture)

[1)] Values are temperature dependant

Security Features

Operation state monitoring mechanism

- Low and high voltage sensors
- Frequency sensors and filters

Memory Security

- ROM code not visible due to implantation
- Internal power-on reset
- 16 bytes security PROM, hardware protected
- Unique chip identification number for each chip
- Security optimized layout and layout scrambling
- MED – memory encryption/decryption device for XRAM, ROM and EEPROM
- True Random Number Generator with Firmware test function
- User settable additional encryption key for EEPROM
- Move code blocking (from EEPROM)
- Additional security features

Anti Snooping

- HW-countermeasures against SPA/DPA-, Timing- and DFA-attacks (differential fault analysis)
- Non standard dedicated Smart Card CPU-Core

Supported Standards

- ISO/IEC 7816
- EMV 2000
- GSM 11.1x
- ETSI TS 102 221
- ISO/IEC 14443

Support

- HW-& SW-Tools (Emulator, ROM Monitor, Card Emulator, Simulator, Contactless Reader EVA Kit, SmartMask™)
- Application notes (e.g.: T=0, T=1, DES, contactless transmission protocol, etc.)

Document References

- Confidential Data Book SLE 66CxxS
- Confidential Instruction SLE 66CxxS
- Confidential Quick Reference SLE 66CxxS
- 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 SCE66
- ROM Monitor SRM66
- Emulator SET66 Hitex or SET66 KSC
- Smart Mask™ Package
- Contactless Reader EVA Kit

Performance DDES-EC2 Accelerator

Operation	Data Block Length	Encryption Time for an 8-Byte Block including Data Transfer
		5 MHz
56-bit Single DES Encryption	64 bit	23 µs
112-bit Triple DES Encryption	64 bit	35 µs
	Operand Length	Calculation Time
		5 MHz
Elliptic Curves GF(2^n) EC-DSA Signature Generate	163 bit	436 ms
Elliptic Curves GF(2^n) EC-DSA Signature Verify	163 bit	1017 ms

Table 1 Ordering Information

Type	Package	Voltage Range	Temperature Range	Frequency Range
SLE 66CL160S – M8.4	M8.4	2.7 V - 5.5 V	– 25°C to + 70°C	1 MHz – 5 MHz
SLE 66CL160S – C	C			

Production sites:

- Regensburg SLE 66CxxS

Pin Description

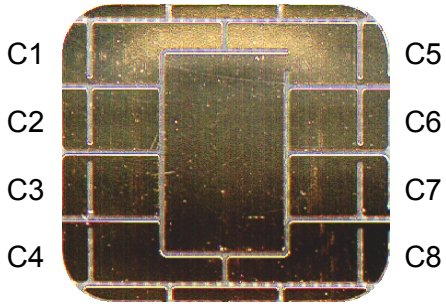

Figure 1 Pin Configuration Wire-bonded Module (top view)

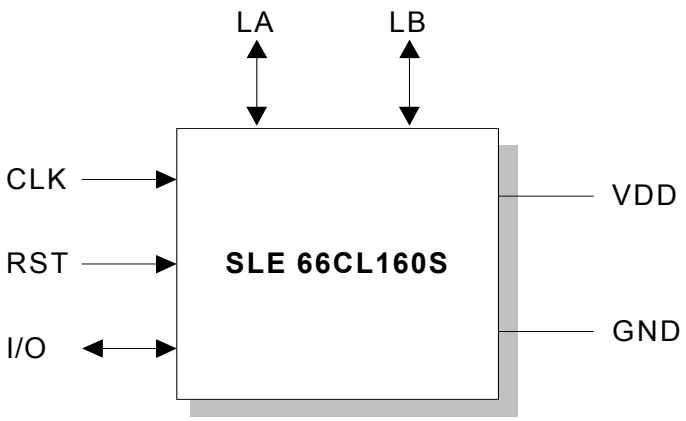

Figure 2 Pad Configuration (die)

Table 2 Pin Definitions and Functions

Card Contact	Symbol	Function
C1	VDD	Supply voltage
C2	RST	Reset input
C3	CLK	Processor clock input
C5	GND	Ground
C7	I/O	Bi-directional data port
	LA	Coil connection pin LA
	LB	Coil connection pin LB

General Description

The dual interface controller SLE 66CL160S is a member of the Infineon Technologies high-end security controller family in 0.6 µm CMOS technology. It contains a contactless and a contact-based interfaces on a single chip and supports symmetric and public-key algorithm such like DES and Elliptic Curve.

The CPU provides the high efficiency of the 8051 instruction set extended by additional powerful instructions with enhanced performance.

The controller offers 31.5 Kbytes of User-ROM, 256 bytes internal RAM, 1 Kbytes XRAM and 16 Kbytes EEPROM. It suits the requirements of the new generation of operating systems.

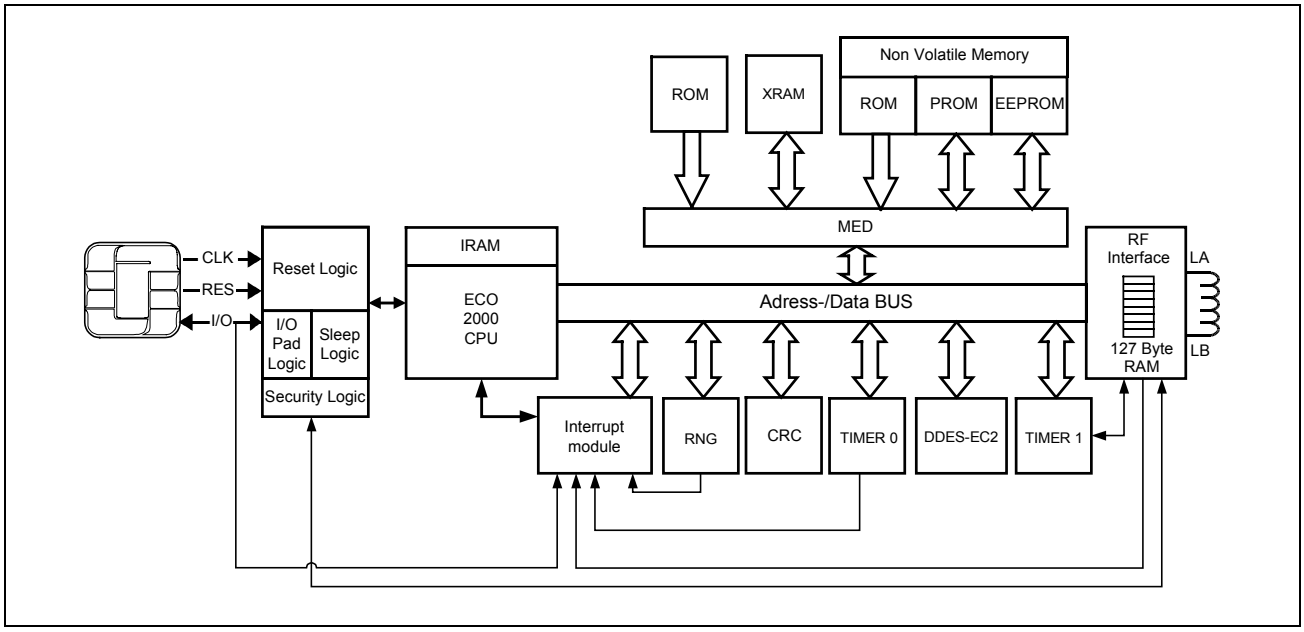

Figure 2: Block Diagram of SLE 66CL160S

In contactless operation, SLE 66CL160S is able to communicate with any Proximity Card Device (PCD) defined in ISO/IEC 14443 such as the Infineon Contactless Reader Evaluation Kit 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 of 106 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.

Different anticollision procedures can be realized in software with the help of one 16-bit timer.

Timers ease the implementation of advanced communication protocols such as T=1 and all other time critical processes for contact-based and contactless communications. An additional interrupt capability of the I/O module allows parallel operation of chip card and terminal.

To minimize the overall power consumption, the chip card controller can be set into sleep mode.

The random number generator (RNG) is able to supply the CPU with true random numbers under all conditions.

The CRC module allows the easy generation of checksums according to ISO/IEC 3309 (16-Bit-CRC).

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. The EC2 module accelerates the multiplication in GF(2^n) and therefore the operations for elliptic curve cryptography.

Additionally, the chip is leading the industry with a new and enhanced level of on-chip security features.

Therefore SLE 66CL160S fulfils the requirements for both contact-based and contactless chip card applications. Especially the field of electronic banking and electronic purses will benefit from the convenient handling and short transaction times achieved by the contactless interface. SLE 66CL160S is a powerful chip card controller integrating outstanding memory sizes, additional peripherals in combination with enhanced performance and optimized power consumption on a minimized die size.