Chip Card & Security ICs

SLE 50C683PE for Mobile Communication

68 Kbyte E²PROM
136 Kbyte ROM
4352 bytes RAM
DES Accelerator

8/16-Bit Security Controller optimized for GSM applications
with enhanced instruction set for large memories
in 0.22 µm CMOS technology

Short Product Information 11.06

SLE 50C683PE Short Product Information	Ref.: SPI_SLE50C683PE_1106
This document contains preliminary information on a new product under development. Details are subject to change without notice.	
Revision History: Current Version 11.06	
Previous Releases:	
Page	

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

Edition 2006

Published by Infineon Technologies AG, AIM 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 optimized for Mobile Communication with enhanced instruction set for large memories in 0.22µm CMOS Technology, 136-Kbytes ROM, 4352 bytes RAM, 68-Kbytes E²PROM, DES Accelerator

General Features

- 8/16-bit microcontroller in 0.22 µm CMOS technology
- Instructions set compatible with standard 8051 processor
- **Defined migration path from SLE66CxxxP/PE products with minimized customer effort based on the same tool set**
- **Dedicated instructions for linear addressing**
- Dedicated, non-standard architecture with **execution time 6 times faster** than standard 8051 core at same external clock. (Up to **18 times faster)**
- **136-Kbytes User ROM** for application programs
- **68-Kbytes E²PROM** for increased memory requirements in mobile applications
- **4-Kbytes XRAM,** 256 bytes internal RAM
- **256 bytes reserved ROM for Resource Management System (RMS) with optimized E²PROM write/erase routines**
- **DES Accelerator**
- **External Clock frequency from 1 up to 7.5 MHz**
- **Internal Clock** with up to 30 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 keep a given power limit
- Two 16-bit Auto-reload Timers with interrupt capability for protocols, security checks & watch dog implementations
- Power saving sleep mode
- **Enhanced UART for handling serial interface** in accordance with ISO/IEC 7816 part 3 **supporting transmission protocols T=1 and T=0**
- CRC Module
- Supply voltage range: 2.7 V to 5.5 V
  (1.8V upon request)
- Support of current consumption limits required by GSM applications
  < 10 mA @ 5.5 V
  < 6 mA @ 3.3 V
  < 4 mA @ 1.98 V (1.8V upon request)
- Operating Temperature range: -25 to +85°C
- Storing temperature range: - 40° to +125°C
- ESD protection larger than 4 kV (HBM)

E²PROM Technology

- Typical programming time (erase & write) including firmware 3 ms
- Fast personalization mode 1 ms per page
- Flexible page mode for 1 to 64 bytes write/erase operation
- 32 bytes security area
- Minimum of 500.000 write/erase cycles @ 25°C per page. Maximum of 16.500.000 write/erase cycles per sector
- Typical data retention of 10 years @ 25°C
- E²PROM programming voltage generated on chip

Security features tailored for mobile applications

- Exception sensors:
  - Voltage sensor
  - Frequency sensor
  - Light Sensor
  - Glitch Sensor
- Life Test for Sensors (UMSLC)
- Bus confusion
- True Random Number Generator
- 16-bit Interrupt Module

Memory Security

- **Memory Management and Protection Unit (MMU)** with application and user defined segments
  - Addressable memory up to 16-MByte
  - Code execution from XRAM possible
- 32 bytes security PROM, hardware protected for batch-, wafer-, die-individual security data. Unique chip identification number for each chip
- MED – memory encryption/decryption device for XRAM, ROM and E²PROM
- Fast IRAM erase
- Enhanced Error correction unit (ECU) controlled by OS

Anti Snooping

- Basic countermeasures against side-channel attacks
- Dedicated Smart Card micro-architecture
- Hardware countermeasures controlled by True Random Number Generator
- Internal oscillator

Document References

- Confidential Data Book
- Confidential Quick Reference
- Chip Qualification report
- Chip delivery specification for wafer with chip-layout (die size, orientation, ...)
- Module specification containing description of package
- Module Qualification report

Development Tools Overview

- Software Development Kit SDK CC
- ROM Monitor & Emulator with stand alone functionality for ROM mask qualification in the end user system
- Flash sample cards for chip evaluation
- Worldwide Application Engineer Team & customer dedicated Field Application Engineers
- Regular Customer trainings on Hardware & Software Tools, Controllers Cryptography, Contactless and Dual interface controllers including ISO/IEC 14443 related topics
- On-site trainings available on request

Supported Standards

- ISO/IEC 7816
- GSM 11.11, 11.12, 11.18
- ETSI TS 102 221

Ordering Information

Type	Package[1]	Voltage Range	Temperature Range	Frequency Range (ext. clock frequency)
SLE 50C683PE C	Die (sawn, unsawn)	2.7 V - 5.5 V or 1.62 V - 5.5 V (upon request)	– 25°C to + 85°C	1 MHz - 5 MHz or 1 MHz – 7.5 MHz
SLE 50C683PE MXXX	MFC5.X (Wire-bonded modules upon request)			

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

Pin Description & Module

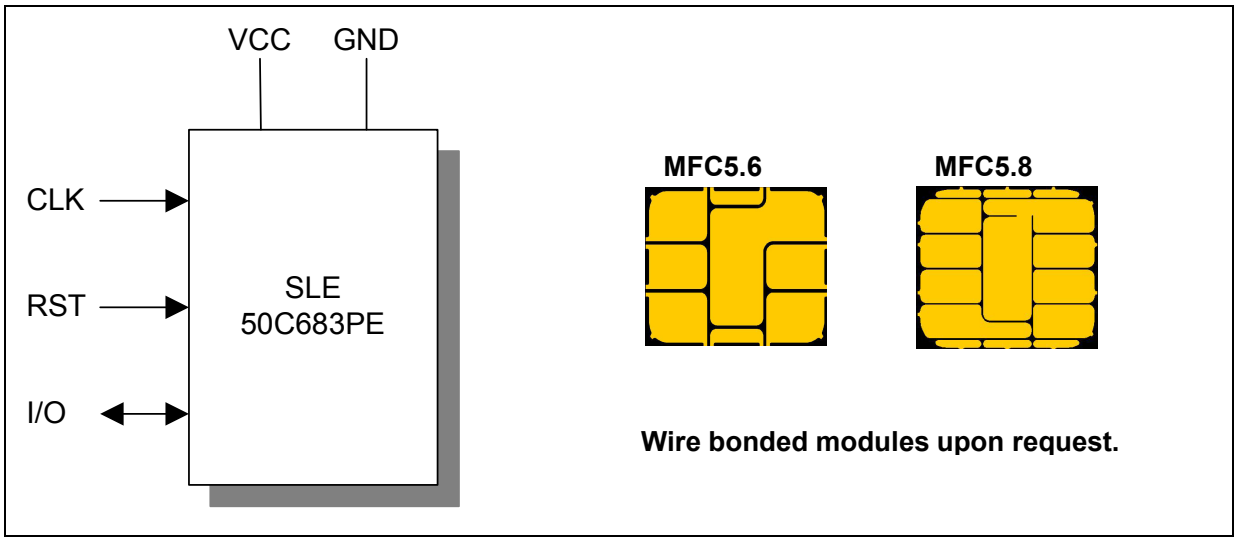

Figure 1: Pin Configuration

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 SLE50C683PE is a member of the streamlined SLE50PE-series of Infineon Technologies optimized for mobile communications. This security controller is manufactured in advanced 0.22 µm CMOS technology. It has a defined migration path from existing 66P/66PE products with minimized customer effort to migrate the OS and is based on the same tool set. The efficiency of the 8051 instruction set extended by additional powerful instructions together with optimized memory sizes, performance and features compared to existing SLE66CxxxPE derivatives.

Performance

The internal clock frequency can be adjusted to a level up to 30 MHz either as a multiple of 1,2,3,4 of 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.
- Automatically adjusted frequency to keep a given maximum power consumption, for GSM requirements.

Memory

The SLE50C683PE offers 136-Kbytes of User-ROM, 256 bytes internal RAM, 4096 bytes XRAM and 68-Kbytes MicroSlim E²PROM, to fulfill requirements of GSM applications.
The large ROM size allows to place applications in ROM 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.
68-Kbytes of E²PROM may contain SIM Application Toolkit, Wireless Application Protocol (WAP), WML-Browser and JavaCard API implementations in NVM.

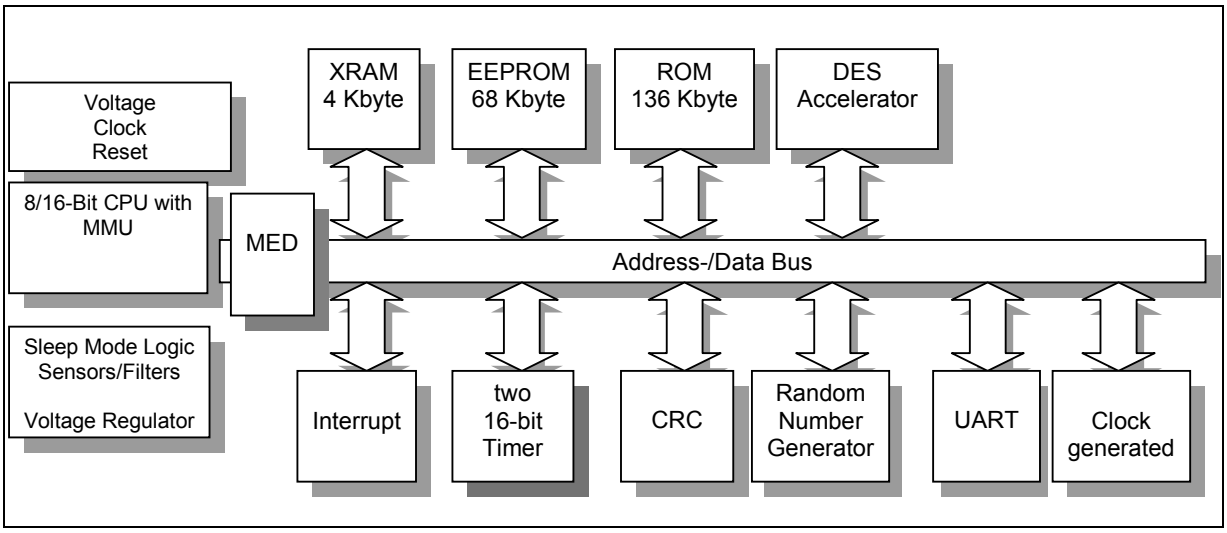

Figure 2: Block Diagram SLE 50C683PE

The new platform is designed to address up to 16 Mbyte. In addition, new instructions have been implemented in the design for an efficient direct access of physical memory ≥ 64 Kbyte.

Security

The set of security features has been tailored to fit to the requirements of mobile communication purposes combined with enhanced reliability for these applications.

- Encrypted storage of any confidential code, data and keys is supported.
- Basic protection against side channel attacks such as: Simple Power Analysis (SPA) , Differential Power Analysis (DPA),
- Basic protection against Differential Fault Analysis (DFA)

Peripherals

The enhanced CRC module allows the easy generation of checksums according to ISO/IEC 3309 (16-Bit-CRC) and offers a loadable initialization vector for a better Java support.

In order to minimize the overall power consumption, the chip card controller IC offers a sleep mode.

The improved UART supports the half-duplex transmission protocols T=0 and T=1 according to ISO/IEC 7816-3 as well as a larger FIFO. 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.

In conclusion, the SLE 50C683PE fulfills all requirements of today's chip GSM Smart Card applications. In addition it offers a powerful platform for multi application cards based on Java.

The SLE 50C683PE integrates outstanding memory sizes, additional peripherals 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