Chip Card & Security ICs

SLE 88CFX4000P for High-End Security Applications

400 Kbyte Flexible EEPROM
16 Kbyte RAM

32-Bit ROM-less microcontroller tailored for high-end security applications with powerful Memory Management & Protection Unit and 1408-bit Crypto Engine (Crypto@1408)
designed in 0.13µm CMOS Technology

Certified Common Criteria EAL5+ (BSI-PP-0002)

Preliminary
Short Product Information 07.06

SLE 88CFX4000P Short Product Information	
This document contains preliminary information on a new product under development. Details are subject to change without notice. **Revision History: 10.04 Current Version: 07.06**	
Previous Releases: SLE 88CFX4000P Preliminary Short Product Information	
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 ICs security.chipcard.ics@infineon.com

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.

32-Bit smartcard microcontroller from the SLE 88 Family, tailored for high-end security applications, manufactured in the advanced 0.13µm CMOS technology, including 400 Kbytes EEPROM with Flash functionality, 16 Kbytes RAM and 1408-bit Crypto Engine (Crypto@1408).

General Features

- **Dedicated smart card core**: pipelined **32-Bit RISC** microcontroller in 0.13 µm CMOS technology with Integral Security Concept
- **Ultra low power consumption design**
- **Very fast application switch**
- **CPU supplied by 2 Cache Memories** (instruction fetch and data access):
  1K Instruction Cache
  2K Data Cache
- **Virtual Machine Acceleration:** specific instruction set for Virtual Machine implementation (Java Card™, MULTOS™, ...)
- 4 Gbytes virtual address range controlled by the powerful **Memory Management and Protection Unit (MMU)**
  - Package Concept: up to 256 packages with different access rights
  - Access rights controlled by hardware firewall and hardware components
  - Controlled access to peripherals and hardware components
- **Interrupt and Trap Control System**
- Memory protected by **Hardware Error Correction Code** for ROM, RAM and EEPROM
- **Optimized Power Management:**
  - Internal clock generation up to 66 MHz
  - Automatic internal adjustment of internal clock according to power classes A,B,C
  - PLL mode
- **400 Kbytes EEPROM**, freely configurable in code/data memory spaces, for application programs and data.
  Examples:
  272 Kbytes of code and 128 Kbytes of data or
  321 Kbytes of code and 79 Kbytes of data
- **16 Kbytes RAM** for local variables, buffers, and stacks
- **80 Kbytes hidden ROM** reserved for the Platform Support Layer (PSL) and STS

E²PROM Technology

- **Min. 500,000 write/erase cycles per page**
- **Max. 16,500,000 write/erase cycles per 4k sector**
- **Data retention: min. 10 years** @ 25°C
- **Erase cycle time 1,3 ms**
- **Write cycle time 1 ms**
- EEPROM programming voltage generated on chip
- Programming while I/O receiving
- Page programming up to 128 bytes at one shot
- Sector erase in one shot
- **Flash personalization time < 10 s**

Security features tailored for high-end applications

- Sensors/Filters:
  - Low and high voltage sensors
  - Low and high frequency sensors
  - Temperature sensor
  - Glitch sensor
  - Light sensor
  - Detection of forbidden states sensor
  - User mode Sensor Life Control
  - Spike filter for CLK
  - Reset filter
- Hardware Memory Management and Protection Unit
- Watch Dog Timer for sensors initialization
- Unique chip identification number for each chip
- Security optimized layout
- Hardware encryption of memories. On-chip encryption of core-internal data.

Peripherals

- **1408-bit Crypto Engine (Crypto@1408)** for fast execution of public key crypto algorithms
  - Optimized for RSA and Elliptic Curves GF(p) and GF(2^m)
  - 1408-bit internal register length
  - Key lengths up to 2048-bit
  - Dedicated 704 bytes of crypto-coprocessor RAM
- **Hardware DES Accelerator**
  - Optimized DES and 3DES calculation
  - Flexible key management
- **True Random Number Generator** (TRNG), AIS-31 compliant
- **Three 16-bit Timers**
- Dedicated smartcard **Hardware UART**: Half-duplex serial I/O interface, support for T=0, T=1, support of division factor up to 16

PSL

- **Ready to use low level software** drivers located in hidden ROM supporting Crypto@1408, UART, Protocol, Timer, RNG, DES, etc…
- **Certified EAL5+ according to BSI-PP-0002 protection profile**
- Certified RNG driver AIS-31
- 1024-bit and 2048-bit crypto libraries
- Application notes and program examples delivered with the SDK

Electrical Characteristics

- Pin configuration and serial interface in accordance with ISO 7816
- Power saving sleep mode (< 100 µA)
- External clock frequency: 1 to 10 MHz
- Supply voltage range: 1.62 V to 5.5 V
- Current consumption: 0.35 mA/MHz
- Temperature range: -25°C to +85°C
- ESD protection > 6 kV (MIL-Standard, HBM)

Support

- **E**mbedded **D**evelopment **E**nvironment (Windows 2000™, XP™) for software development and validation
  - Simulator for functional debugging
  - Emulator for real-time debugging
  - Flash samples for rapid prototyping
  - Flash loader tools for personalization environments
- Programmer's Manual with application notes (e.g.: T=0, T=1, 3DES, AES, RSA, Elliptic Curves, SHA1, CRC etc.)
- Dedicated trainings from beginner to expert level

Features (cont'd)

Enhanced Crypto Performance

Crypto@1408 Library Run Times					
Operation	**Modulus**	**Exponent**	**Run time (ms)**		
			5 MHz	**33 MHz**	**66 MHz**
RSA KeyGen	1024 bit	1024 bit	13200	2000	1000
RSA Sign (with CRT)	1024 bit	1024 bit	184,8	28	14
RSA Verify	1024 bit	F_4	26,4	4	2
RSA KeyGen	2048 bit	2048 bit	52600	8000	4000
RSA Sign (with CRT)	2048 bit	2048 bit	765,6	116	58
RSA Verify	2048 bit	F_4	343,2	52	26

Notes:

1. Crypto@1408 works independently of I/O operations or DES calculations.
2. The run times are typical measured values **including countermeasures and data transfers from/to CPU.**
3. The Key Generator values give the average run time.

Ordering Information

Type	Package[1]	Voltage Range	Temperature Range	Frequency Range (ext. clock frequency)
SLE 88CFX4000P C	Die (sawn, unsawn)	1.62 V - 5.5 V	– 25°C to + 85°C	1 MHz - 10 MHz
SLE 88CFX4000P MXXX	M5.X MFC5.X DSO-20			

[1] available as flip chip module (MFC), wire-bonded module (M5) , die (C) or as DSO for customer packaging

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

Pin Description & Module

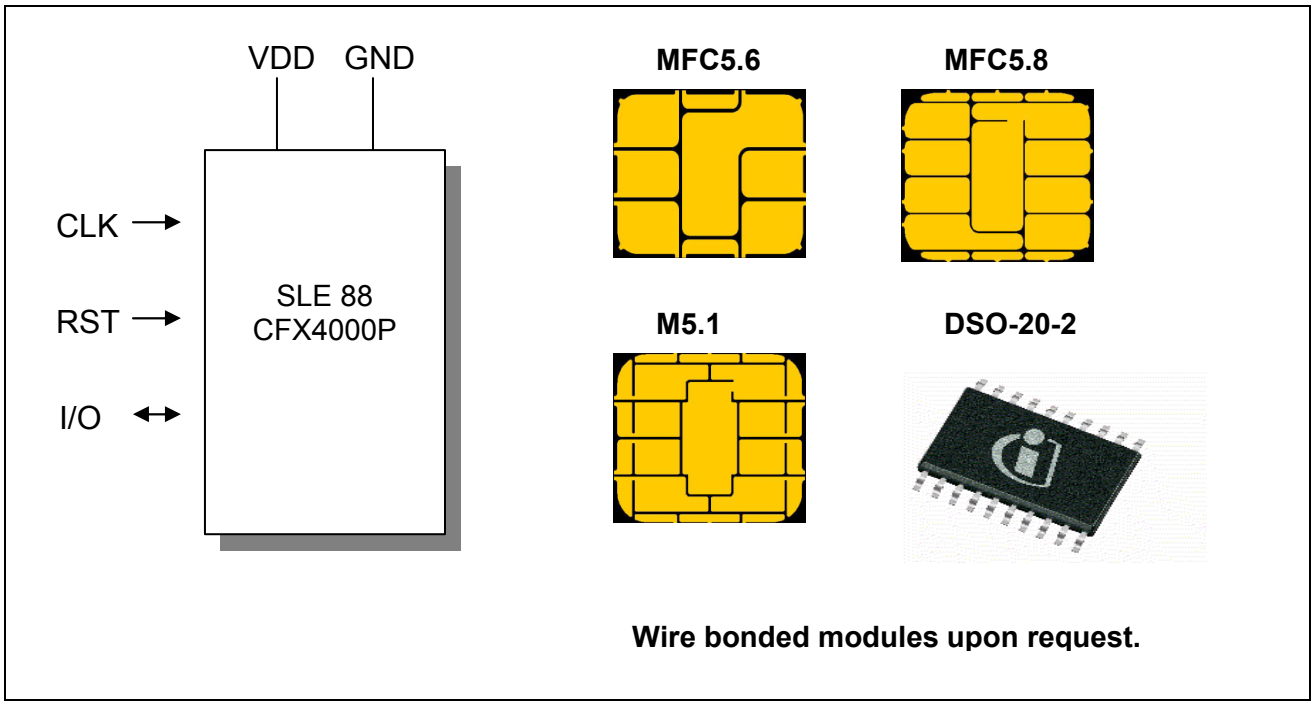


Figure 1: Pin Configuration

Pin Definitions and Functions

Pin symbol	Function
VDD	Operating voltage
RST	Reset input
CLK	Processor clock input
GND	Ground
I/O	Mono and bi-directional data ports

General Description

The SLE 88CFX4000P is the first smartcard microcontroller on the market in 0.13µm CMOS technology. In this product family, Infineon Technologies realises increased security and performance while reducing power consumption, and additionally provides a platform for real multi-application (i.e. several applications can run and coexist securely on the card).
As flash device, the SLE 88CFX4000P offers full lead time and configuration management flexibility for a best time to market performance. A broad range of hardware and software based development tools offers to the user the means for high-end operating system development and validation. The PSL provides all device drivers necessary to use the chip resources and peripherals such as optimum EEPROM programming, memory management, crypto implementations, and many others. It also allows an easier and faster code implementation on a high level, without detailed knowledge of the hardware, and independently of its eventual changes and evolutions. As a consequence, porting an existing code from a derivative of the SLE 88 Family to another is easy and quick.
The SLE 88CFX4000P fully meets the requirements for real multi-application operating systems. It allows secure operation of banking, access control, loyalty, GSM/USIM, Pay-TV, health care and identification applications all in one chip. The advanced 0.13µm technology, the Integral Security Concept, the low power optimised 32-bit core supported by various powerful peripherals, and the possibility to adapt the performance to application requirements establish the foundation for a completely new chip card generation.

Performance and Virtual Machine Acceleration

Performance is first of all enhanced by the 32-bit architecture that processes instructions and data 32-bit wise. This is supported by the implementation of cache memories in the core that allow faster access to instructions and data. Performance is also enhanced by a clock frequency of up to 66MHz. And finally, efficient support and an additional performance increase of multi-application schemes are gained by a hardware acceleration of Virtual Machine Languages like Java Card™ or MULTOS™.

The SLE 88CFX4000P includes an intelligent power management module that covers the voltage classes A, B and C of the GSM and the 3rd generation specification for mobile communication standards.

Memory

The 32-bit architecture allows the linear addressing of large memories for a more convenient code implementation. With the 0.13µm process, the SLE 88CFX4000P offers large on-chip memories with 80 Kbytes of ROM, 400 Kbytes of EEPROM, and 16 Kbytes of RAM. The ROM is reserved for the Platform Support Layer (PSL) and the Self Test Software (STS) that are provided by Infineon Technologies, so that these lower code layers do not occupy the user memory space. The large EEPROM space is the basis of Infineon Technologies “Flash” Concept where the entire EEPROM is freely configurable in code and data sections, and so it can be used to store Operating System, as well as application code and data. Each application can be tailored to fit its targeted project. This customization provides added value to the system and the possibility to serve multiple projects with the same platform. The 400 Kbytes EEPROM are e.g. configurable as 256 Kbytes of code and 144 Kbytes of data or 321 Kbytes of code and 79 Kbytes of data. This concept offers the flexibility and convenience of Flash memory, but takes advantage of the EEPROM cell quality (timing, cycling and endurance).

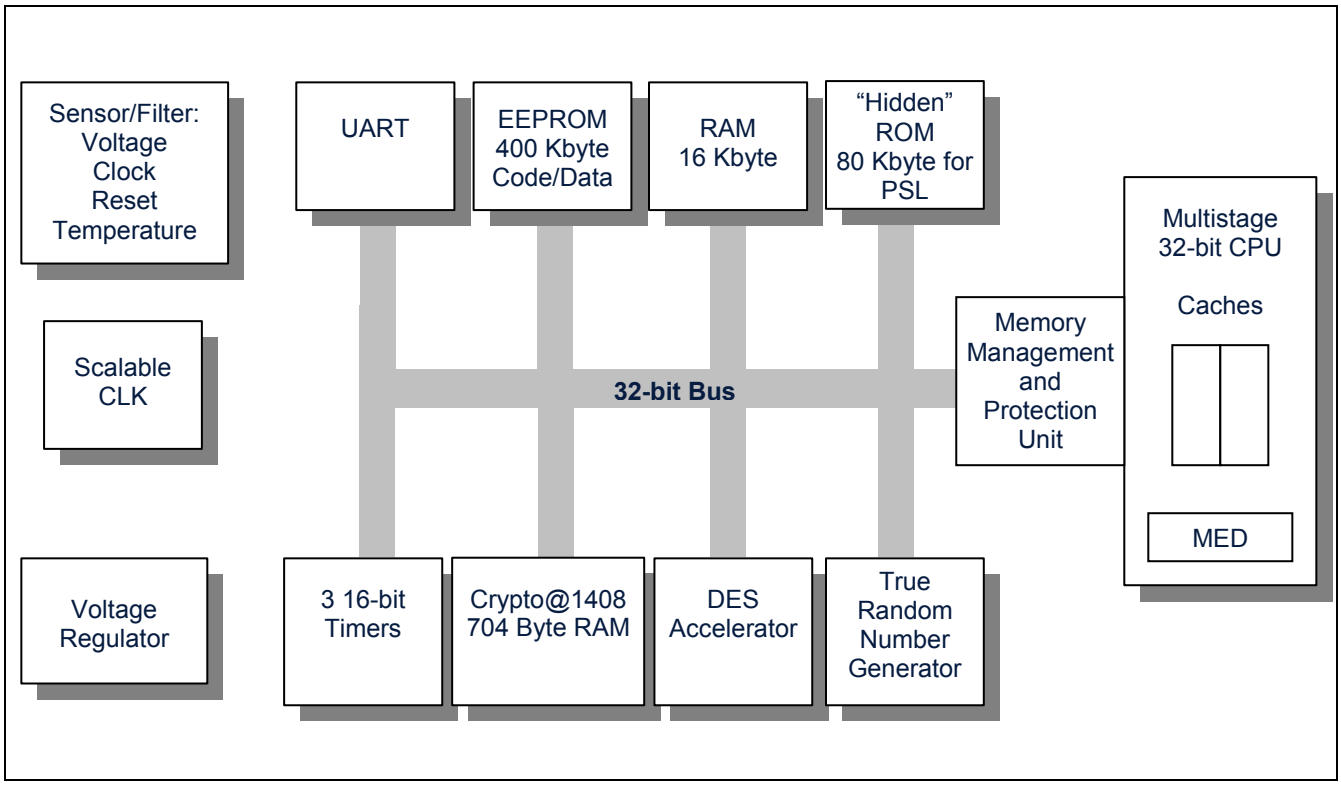
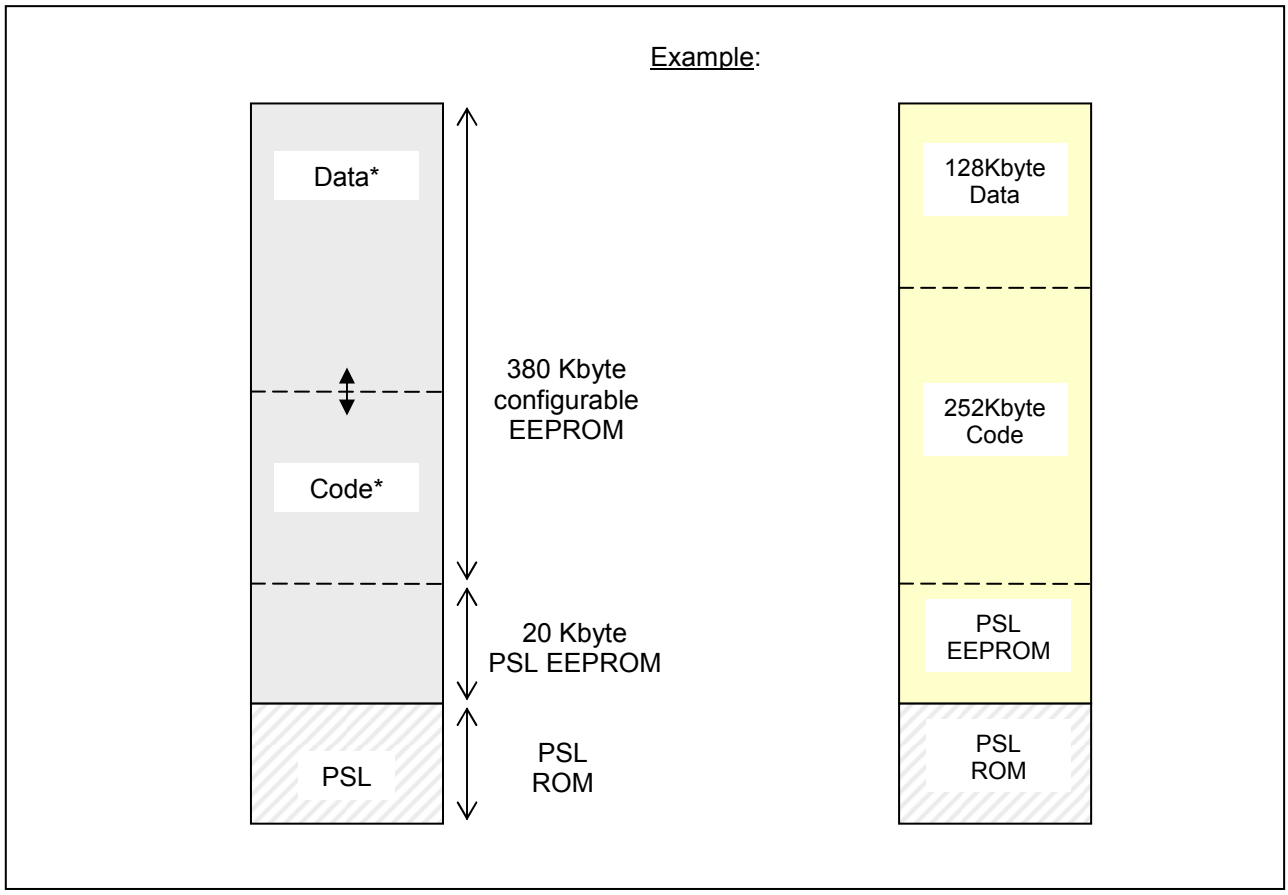


Figure 2: Block Diagram SLE 88CFX4000P

Memory



*Note: The Data and Code sectors includes about 3% mapping storage

Figure 3: Memory configuration

The Memory Management and Protection Unit (MMU) handles a virtual address range of 4 Gbytes, and serves as a hardware firewall to enable secure separation of adjacent application codes and data. A very efficient context/application switching mechanism allows fast switching between multiple tasks. Program and data modules are organised as packages. And each package has a defined memory range of 16 Mbytes with dedicated access rights for memories and peripherals. The flexible MMU concept also shortens development cycles for additional applications.

Security

An innovative security concept has been created that is based on the entire integration of security measures at each hardware and software design phase of the SLE 88 Family. With this Integral Security Concept, the SLE 88 takes a quantum leap in terms of improved on-chip security. It has reached certification is Common Criteria level EAL5+ according to protection profile BSI-PP-0002 in March 2006.

Peripherals

A number of powerful peripherals offer hardware support for time and code intensive operations.

The Crypto@1408 is equipped with its own RAM of 704 bytes and supports all of the known public-key algorithms based on large integer modular arithmetic with configurable register lengths of up to 1408 bits. It allows fast and efficient calculation of e.g. RSA operations with key lengths up to 2048-bit but also Elliptic Curves over GF(p) as well as GF(2^m). For symmetric crypto operations, a DES accelerator supporting also Triple-DES is implemented. Using the Crypto@1408 and DES module a secure transmission for downloading of additional applications can be ensured.

The UART supports the chip card protocols T=0 and T=1 and is also able to manage full-duplex data transfer.

The True Random Number Generator (TRNG) is able to supply the CPU with true random numbers whose quality is ensured according to AIS-31 strict evaluation guidelines.

An interrupt control unit supports a programmable interrupt system with UART, timers, and the other peripherals as interrupt sources.

A variety of different trap vectors informs the operating system about exceptions (e.g. access violation).

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.
CC EAL 5+	Common Criteria Certification level
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
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
MED	Memory Encryption Decryption
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