Security & Chip Card ICs

SLE 88CFX4002P

32-Bit Multi Application Security Controller
with powerful Memory Management & Protection Unit
in 0.13µm CMOS Technology,
240 Kbytes ROM, 400 Kbytes configurable EEPROM,
16 Kbytes RAM, and 1408-bit Crypto Engine (Crypto@1408Bit)

Preliminary Short Product Information 01.04

SLE 88CFX4002P Preliminary Short Product Information	
This document contains preliminary information on a new product under development. Details are subject to change without notice.	
Revision History: Current Version 01.04	
Previous Releases: -	
Page	Subjects (changes since last revision)

Important: Further information is confidential and on request. Please contact:
Infineon Technologies AG in Munich, Germany,
Secure and Mobile Solutions - Security Group
Fax +49 89 234-81000

Published by Infineon Technologies AG, Secure and Mobile Solutions - Security Group
St.-Martin-Strasse 76, D-81541 München

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 Multi Application Security Controller with powerful Memory Management and Protection Unit in 0.13µm CMOS Technology, 240 Kbytes ROM, 400 Kbytes configurable EEPROM, 16 Kbytes RAM and 1408-bit Crypto Engine (Crypto@1408Bit)

Features

- **Dedicated smart card core**: pipelined **32-Bit RISC** micro-controller in 0.13 µm CMOS technology with Integral Security Concept
- Designed for maximum security and maximum performance at ultra low power consumption
- Instruction set acceleration of Virtual Machine languages (e.g. Java Card™, MULTOS™, ...)
- 4 Gbytes address range controlled by a powerful **Memory Management and Protection Unit (MMU)**
  - Package Concept: application oriented memory partitioning
  - Secure hardware controlled execution of applications and application data access
  - Controlled access to peripherals
  - Hardware Error Correction Code for ROM, RAM and EEPROM
- Efficient Task switch capability
- **80 Kbytes of reserved ROM** for the Platform Support Layer (PSL) and STS
- **160 Kbytes of User ROM** for libraries, operating system and applications
- **400 Kbytes of EEPROM**, software configurable in code/data memory spaces with 4 Kbytes granularity, for application programs and data.
  Example:
  272 Kbytes of code and 128 Kbytes of data or
  144 Kbytes of code and 256 Kbytes of data
- **16 Kbytes of RAM** for local variables, buffers, and stacks
- **1K and 2K high performance Instruction and Data Cache Memories** for instruction fetch and data access
- **Internal clock generation**
  Adjustment of internal clock according to available power and required performance:
  - Increase internal clock for maximum speed (66 MHz)
  - Reduce internal clock for lowest power consumption

Integral Security Concept

- Hardware Memory Management and Protection Unit
- Enhanced on-chip encryption of internal data
- Low and high voltage sensors
- Low and high frequency sensors
- Spike filter for CLK
- Reset filter
- Temperature sensor
- Glitch Sensor
- Light Sensor
- Watch Dog Timer for sensors initialization
- User mode Sensor Life Control
- Detection of forbidden states sensor
- Unique chip identification number for each chip
- Security optimized layout
- Hardware encryption of memories
- Targeted certification: Common Criteria level EAL5+

Features (cont'd)

EEPROM

- Self timed programming
- **500,000 write/erase cycles per page**
- Data retention: min. 10 years @ 25°C
- EEPROM programming voltage generated on chip
- Erase cycle time 1,3 ms
- Write cycle time 1 ms
- Page mode for programming up to 128 bytes at one shot

Peripherals

- **1408-bit Crypto Engine (Crypto@1408Bit, formerly Crypto2000)** for fast execution of public key crypto algorithms
  - Optimized for RSA and Elliptic Curves GF(p) and GF(2^m)
  - Key lengths up to 2048-bit
  - Dedicated 880 bytes of crypto-coprocessor RAM
- **DES Accelerator**
  - DES and 3DES in hardware
  - Flexible key management
  - Optimized for data throughput (parallel load)
- **True Random Number Generator** (TRNG), AIS-31 compliant
- Three 16-bit Timers
- Dedicated smart card UART, two I/O ports (IO1 and IO2), half and full duplex transmission, support for T=0, T=1
- **Platform Support Layer (PSL)** including device drivers for RNG, DES, Crypto@1408Bit, EEPROM, etc.

Electrical Characteristics

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

Support

- **I**ntegrated **D**evelopment **E**nvironment (Windows 2000™, NT™ and UNIX Workstation) for high-end software development and validation
  - Integrated simulator / debugger
  - Emulator for real-time debugging
- Programmer's Manual with application notes (e.g.: T=0, T=1, 3DES, AES, RSA, Elliptic Curves, SHA1, CRC etc.) and software developer guidelines
- C libraries (e.g. Crypto library)

Features (cont'd)

Best Crypto Performance

Operation	Modulus	Exponent	Crypto@1408Bit Perf. at 5MHz [ms]	Crypto@1408Bit Perf. at 66MHz [ms]
RSA signature (without CRT)	512 bit	512 bit	53	4
RSA signature (without CRT)	1024 bit	1024 bit	238	18
RSA signature (without CRT)	2048 bit	2048 bit	25.080	1.900
RSA signature (with CRT)	1024 bit	1024 bit	53	4
RSA signature (with CRT)	2048 bit	2048 bit	475	35
RSA verification	1024 bit	32 bit	8	0,5
RSA verification	2048 bit	F_4	132	11
RSA Key Generation (n=5)	1024 bit		4.356	330
RSA Key Generation (n=5)	2048 bit		35.640	2.700
EC DSA over GF(p) signature	160 bit	160 bit	99	8
EC DSA over GF(p) verification	160 bit	160 bit	198	15
EC DSA over GF(2^n) signature	160 bit	160 bit	158	12
EC DSA over GF(2^n) verification	160 bit	160 bit	317	24

Notes:

- Crypto@1408Bit works independently of I/O operations or DES calculations.
- n is the number of Miller-Rabin rounds

Pin Description

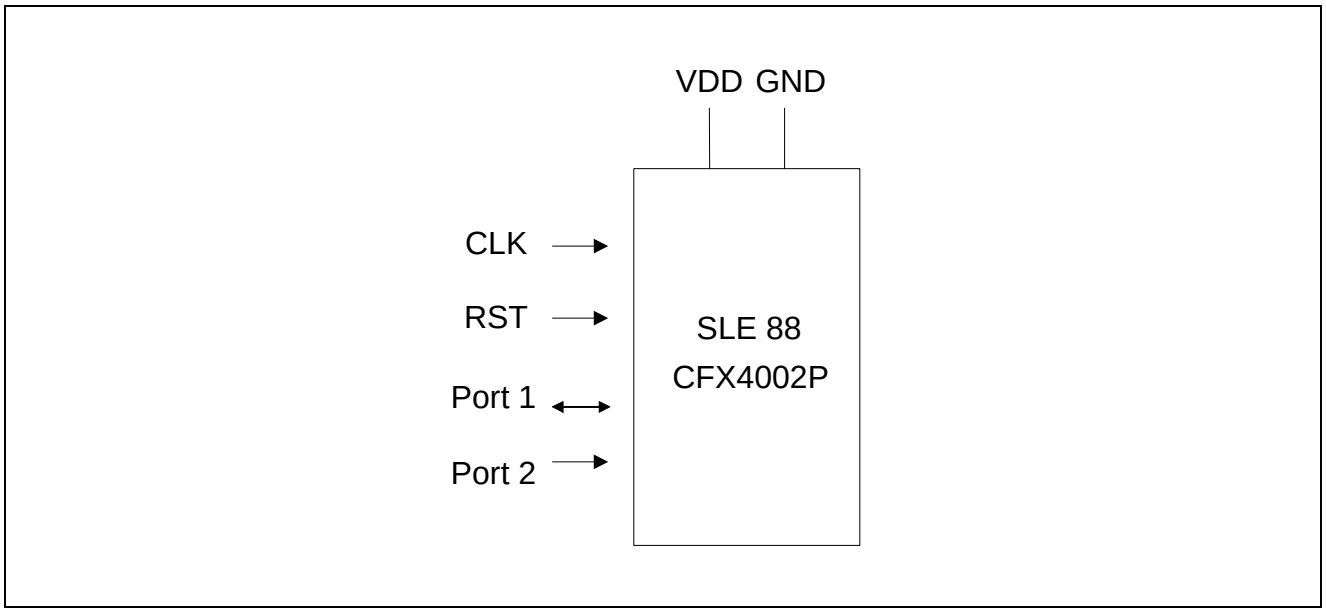

Figure 1: Pin Configuration

Pin Definitions and Functions

Pin symbol	Function
VDD	Operating voltage
RST	Reset input
CLK	Processor clock input
GND	Ground
Port 1, 2	Data ports

Block Diagram

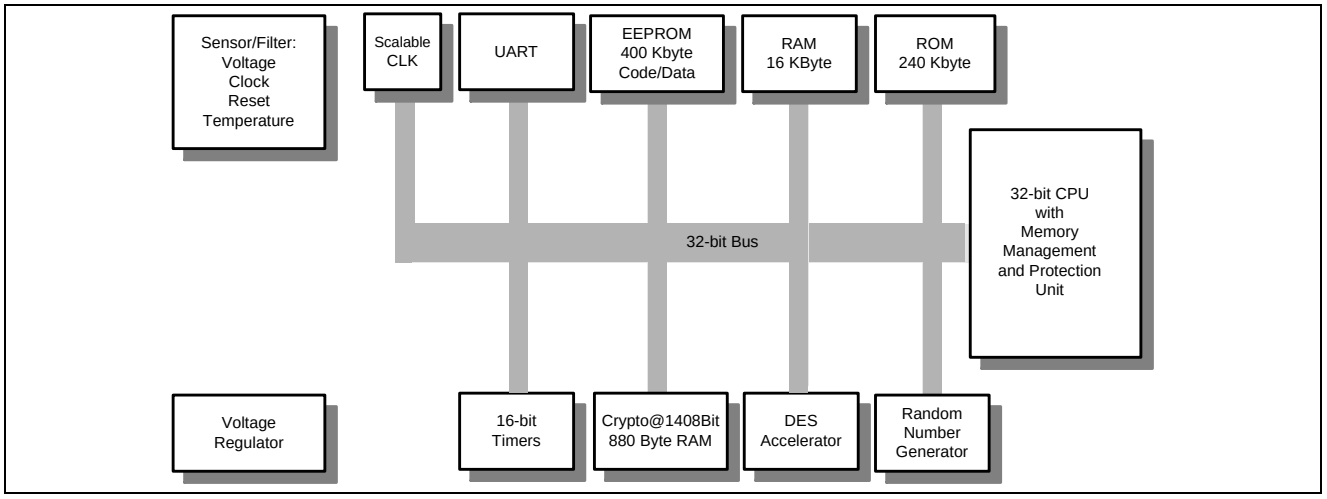

Figure 2: SLE 88CFX4002P, 32-bit CPU and Peripherals

General Description

SLE 88CFX4002P is the most sophisticated smart card microcontroller on the market. It is manufactured in 0.13 micron CMOS technology and only differs from SLE 88CFX4000P in its additional 160 Kbytes User ROM. In this product family, Infineon Technologies realises increased security and performance while reducing power consumption, and additionally provides a platform for real multi-application and multi-tasking operating systems.

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™.

Large Memories

The 32-bit architecture allows the linear addressing of large memories for a more convenient code implementation. With the 0.13 micron process, SLE 88CFX4002P offers largest on-chip-memories with 240 Kbytes of ROM (160 Kbytes User ROM and 80 Kbytes reserved ROM), 400 Kbytes of EEPROM, and 16 Kbytes of RAM. The separate 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 configurable in code and data sections with 4Kbytes granularity, and so it can be used to store Operating System program code and data, 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 400K EEPROM are e.g. configurable as 256 Kbytes of code and 144 Kbytes of data or 320 Kbytes of code and 80 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).

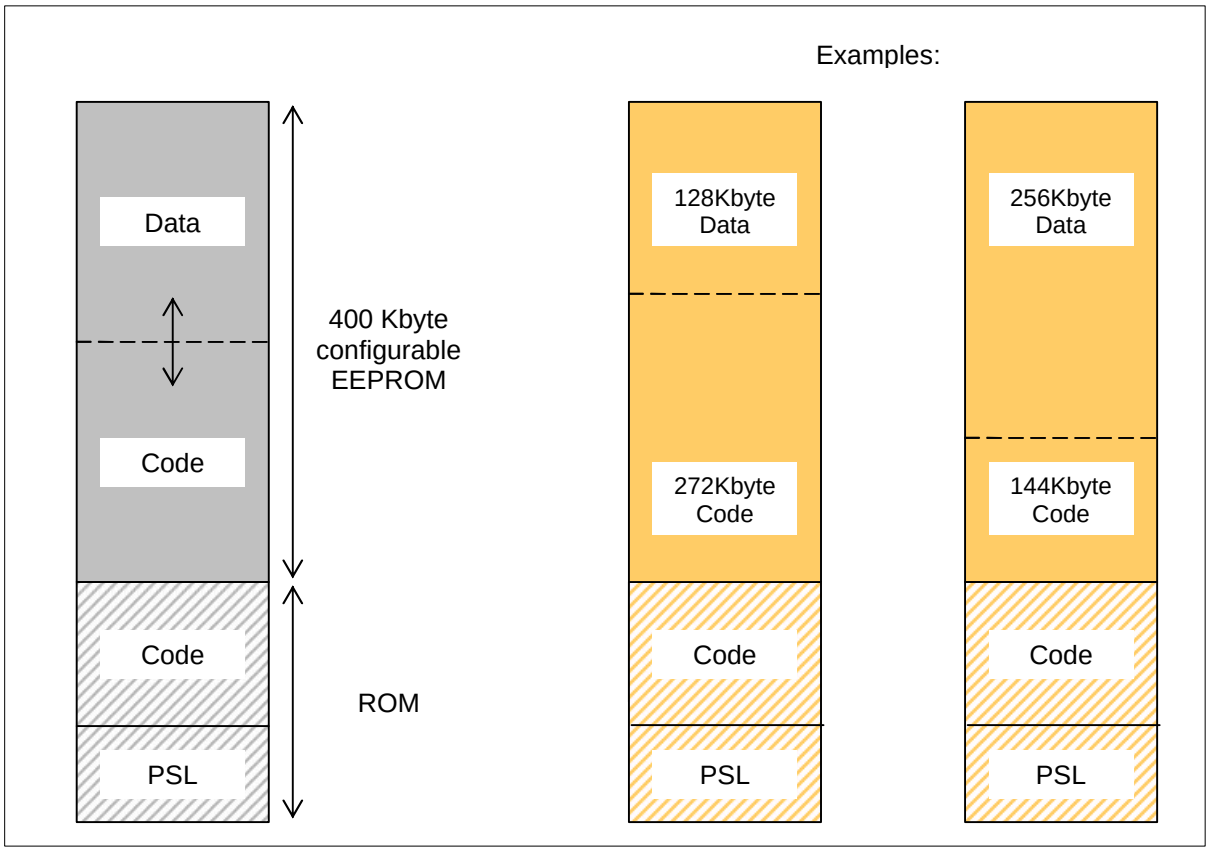

Figure 3: Memory configuration

Real Memory Management Unit

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. It furthermore enables the secure downloading of applications in the field.

Power Consumption

SLE 88CFX4002P includes an intelligent power management module that covers the voltage classes A, B and C of the 3rd generation specification for mobile communication TS102 221.

Peripherals

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

The Crypto@1408Bit is equipped with its own RAM of 880 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). A 1024-bit RSA signature with Chinese Remainder Theorem can be performed in 4ms at 66MHz. For symmetric crypto operations, a DES accelerator supporting also Triple-DES is implemented. A Triple-DES can be performed in 1.5 microseconds at 66MHz. Using the Crypto@1408Bit 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).

Security

As security is Infineon first priority, an innovative security concept has been created that is based on the entire integration of security measures in the SLE88 at each design phase of the core, architecture and modules, at every level, and does not exclusively rely on the addition of security features to an existing system. With this Integral Security Concept, the SLE 88 takes a quantum leap in terms of improved on-chip security. Targeted certification is Common Criteria level EAL5+.

Support

A broad range of hardware and software based development tools offers to the user the facilities for high-end operating system development and validation. The PSL provides all devices 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 SLE88 family to the other is easy and quick.

Conclusion

SLE 88CFX4002P 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 0.13 micron 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 era.

Glossary

AES	Advanced Encryption Standard, successor of DES.
AIS-31	*Anwendungshinweise und Interpretation zum Schema*: 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*
IO	Input/Output
Miller-Rabin	Test for prime numbers.
Modulus	Component of RSA key
RAM	Random Access Memory
RISC	Reduced Instruction Set Computer
RNG, TRNG	Random Number Generator, True Random Number Generator
PSL	Platform Support Layer
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