Security & Chip Card ICs

SLE 88CX720P

32-Bit Multi Application Security Controller
with powerful Memory Management & Protection Unit
in 0.22µm CMOS Technology,
240 Kbytes ROM, 8 Kbytes RAM, 80 Kbytes EEPROM
and 1100-Bit Advanced Crypto Engine

Preliminary Short Product Information 06.03

SLE 88CX720P 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 06.03	
Previous Releases: 04.03	
Page	Subjects (changes since last revision)
3/8, 7/8	WPSC ™ occurrences deleted.
4/8	Tools support on Windows 2000™ added.

Important: Further information is confidential and on request. Please contact:
Infineon Technologies AG in Munich, Germany,
Security & Chip Card ICs,
Fax +49 89 234-81000

Published by Infineon Technologies AG, CC Applications Group
St.-Martin-Strasse, 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 0.22µm CMOS Technology
240 Kbytes ROM, 8 Kbytes RAM, 80 Kbytes EEPROM and
1100-Bit Advanced Crypto Engine

Features

- **Dedicated smart card core**: pipelined **32-Bit RISC** micro-controller in 0.22 µm CMOS technology with integrated 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 ECC for ROM, RAM and EEPROM
- Efficient Task switch capability
- **240 Kbytes of ROM** for application programs, libraries, and device drivers
- **80 Kbytes of EEPROM** as program and data memory
- **8 Kbytes of RAM** for local variables, buffers, and stacks
- **High performance 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 (55 MHz)
  - Reduce internal clock for lowest power consumption (e.g. contactless conditions)

EEPROM

- Self timed programming
- **500,000 write/erase cycles**
- Data retention: min. 10 years @ 25°C
- EEPROM programming voltage generated on chip
- Erase/Programming cycle time 4.5 ms
- Page mode for programming up to 64 bytes at one shot

Integrated Security Concept

- Hardware Memory Management and Protection Unit
- Enhanced on-chip encryption of internal data
- Low and high voltage sensors
- High and low frequency sensors
- Spike filter for CLK
- Reset filter
- Temperature sensor
- Glitch Sensor
- Light Sensor
- Unique chip identification number for each chip
- Security optimized layout
- Hardware encryption of memories

Peripherals

- **1100-bit Advanced Crypto Engine (ACE)** for fast execution of public key crypto algorithms
  - Optimized for RSA and Elliptic Curves
  - Key lengths up to 2048-bit
  - Dedicated 700 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** (RNG)
- AIS-31 compliant
- Three 16-bit **Timers**
- Dedicated smart card **UART**, two IO 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, ACE, EEPROM, etc.

Electrical Characteristics

- Pin configuration and serial interface in accordance with ISO 7816
- Power saving sleep mode (down to 100 µA)
- External clock freq.: 1 to 10 MHz
- Supply voltage range: 2.7 V to 5.5 V
- Current consumption
  - 0.5 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 95™, NT™, 2000™ and UNIX Workstation) for high-end software development and validation
  - Integrated simulator / debugger
  - Emulator for real-time debugging
- Hardware Emulator
- Programmer's Manual with application notes (e.g.: T=0, T=1, DES, RSA etc.) and software developer guidelines
- C libraries (e.g. Crypto library)

Features (cont'd)

Enhanced Crypto Performance

Operation	Modulus	Exponent	ACE Perf. at 5MHz [ms]	ACE Perf. at 55MHz [ms]
RSA signature (without CRT)	512 bit	512 bit	110	10
RSA signature (without CRT)	1024 bit	1024 bit	860	78
RSA signature (without CRT)	2048 bit	2048 bit	113.000	10.000
RSA signature (with CRT)	1024 bit	1024 bit	230	25
RSA signature (with CRT)	2048 bit	2048 bit	1.800	170
RSA verification	1024 bit	32 bit	30	3
RSA verification	2048 bit	F_4	628	57
RSA Key Generation (n=5)	1024 bit		17.000	1.560
RSA Key Generation (n=5)	2048 bit		160.000	14.400
EC DSA over GF(p) signature	160 bit	160 bit	260	24
EC DSA over GF(p) verification	160 bit	160 bit	550	50
EC DSA over GF(2^n) signature			---	---
EC DSA over GF(2^n) verification			---	---

Note: The ACE works independently of I/O operations or DES calculations.

Pin Description

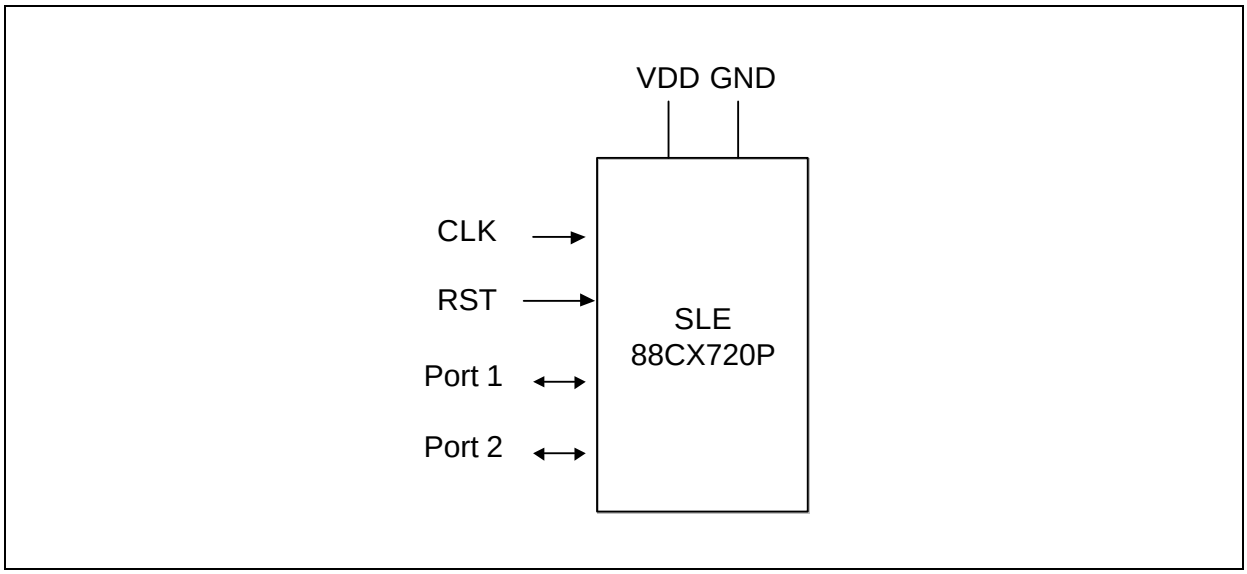

Figure 1: Pin Configuration

Pin Definitions and Functions

Pin symbol	Function
VDD	Operating voltage
RST	Reset input
CLK	Processor clock input
GND	Ground
Port 1, 2	Bi-directional data ports

Block Diagram

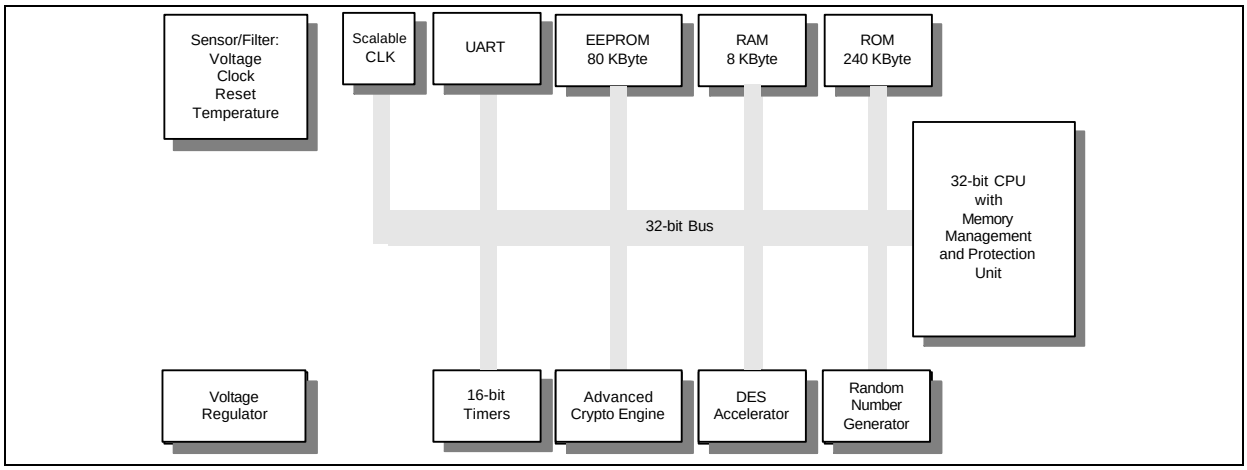

Figure 2: SLE88CX720P, 32-bit CPU and Peripherals

General Description

SLE 88CX720P is the first product of the SLE 88CXxxxP family. This new high-end security controller family in 0.22 µm CMOS technology incorporates a dedicated 32-bit smart card core. In this product family, Infineon Technologies realises increased security and performance while reducing power consumption. Offering high performance at lowest power consumption, the controller family is well suited for both contactless and contact-based applications.

SLE 88CX720P provides a platform for modular multi-application and multi-tasking operating systems. The Memory Management and Protection Unit (MMU) serves as a firewall to enable secure separation of adjacent application programs and data. Furthermore, the MMU is the hardware basis for secure downloading of applications in the field, even after card personalization. A very efficient context/application switching mechanism allows fast switching between multiple tasks. The flexible MMU concept also shortens development cycles for additional applications.

The high execution performance of the CPU is achieved by a smart card dedicated 32-bit RISC core.
Efficient support and an additional performance increase of multi-application schemes is gained by a hardware acceleration of Virtual Machine languages like Java Card™ or MULTOS™.

The SLE 88CX720P is fabricated in a 0.22 micron CMOS process, which allows for largest on-chip memories. We cover the voltage classes B and C of the 3^{d} generation specification for mobile communication TS31.101. The IC offers 240 Kbytes of ROM, 8 Kbytes of RAM and 80 Kbytes EEPROM, in total including PSL. The virtual address range of the MMU is 4 Gbytes. Program and data modules are organised as packages. Each package has a defined memory range of 16 Mbytes and dedicated access rights for memories and peripherals.

Powerful peripherals offer hardware support for time and code intensive operations. The Advanced Crypto Engine (ACE) is equipped with its own RAM of 700 bytes and supports all of the 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. For symmetric crypto operations, a DES accelerator supporting Triple-DES is implemented. Using the ACE 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 Random Number Generator (RNG) is able to supply the CPU with true random numbers. An interrupt control unit supports a programmable interrupt system with UART, timers,

and the other peripherals as interrupt sources. To minimise the overall power consumption the chip card controller IC offers a sleep mode.

As security was the first priority for the new core design, Infineon Technologies integrated an entirely new security concept instead of adding additional security features to an existing design. The SLE 88CX720P takes a quantum leap in terms of improved on-chip security. A variety of different trap vectors informs the operating system about exceptions (e.g. access violation).

A broad range of hardware and software based development tools offers the user the facilities for high-end operating system development and validation.

In conclusion, the SLE 88CX720P 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 0.22µm technology, the highly developed 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.