Chip Card & Security

SLE 88CFX6600P

32-Bit Security Controller
Optimized for multi-application cards with high level of security

660 kBytes Flexible EEPROM
32 kBytes RAM

Common Criteria EAL5+ (high) and EMVCo (targeted)

Short Product Information 12.2009

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

Published by Infineon Technologies AG,
81726 Munich, Germany
© Infineon Technologies AG 2009
All Rights Reserved.

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.

General Features

- **Dedicated 32-bit smartcard core designed in cost-optimized 0.13 µm technology**
  - Pipelined 32-Bit RISC CPU with proprietary instruction set
  - Specific instructions for Virtual Machine implementation like Java Card
- **Ultra low power consumption design**
- **Very fast Task Switching supported by hardware mechanism for pre-emptive multitasking support**
- **Maximum performance**
  - **CPU supplied by 2 Cache Memories** for fast instruction fetch and data access
  - **Internal clock generation up to 33 MHz**
  - **Intelligent Power Manager** which adjusts automatically and efficiently the internal clock according to a dedicated power class
- **Secure multi-application with Memory Management and Protection Unit (MMU)**
  - 256 packages separated and secured by hardware firewalls
  - Data and code access controlled by hardware
  - Memory and peripherals access managed with hardware supervisor components

Memory

- **660 kBytes EEPROM with Flash functionality and free partitioning between code and data**
- **32 kBytes RAM** for local variables, buffers, and stacks

- **Memories encrypted by MED (Memory Encryption/Decryption) device**
- Memories protected by Hardware Error Correction Code

Interfaces

- **Smartcard UART for handling serial interface** in accordance with ISO/IEC 7816 part3 **supporting transmission protocols T=1 and T=0, Support of clock division factor of 8 (PPS97)**

EEPROM Technology

- **Very Fast Programming:**
  - Write/erase time < 2,3 ms
  - Flash functionality with 4k sector flash and erase in one shot
  - EEPROM page programming: 1 to 128 Byte
- **Very High Endurance:**
  - 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

Security Features

- **32-bit Proprietary Instruction Set**
- **Memory and CPU Error Detection, Memory-, Bus- and SFR-Encryption**
- **DPA / SPA**, **DEMA / SEMA countermeasures** incl. Dual Rail Logic
- **Security Sensors** (Voltage, frequency, Light, Temperature, Glitch)
- **Active Shield**
- **True RNG according to AIS31**
- **Memory Management and Protection Unit** with Level Concept
- Chip ID, unique chip identification number for each chip

Coprocessors and Peripherals

- **High Performance Crypto Engine for PKI, RSA, EC calculations**
  - 1408-bit Crypto Engine
  - Dedicated 704 bytes of crypto-coprocessor RAM
  - Optimized for RSA up to 2048 bit and for ECC up to 521 bit (GF(p) and GF(2^m))
- **Hardware DES Accelerator for DES and Triple DES calculations**
- **True Random Number Generator** for true random number generation
- **Pseudo Random Number Generator** for very fast random number generation
- **Three 16-bit Autoreload Timers** for protocol implementation, event monitoring
- **CRC** hardware module for fast CRC calculations

Tools and Support

- **Software Development Kit, SDK 88**
- **FPGA based Emulator** (same as SLE 7x emulator)
- **Flash samples** for immediate test and validation, enabling short Time-to-Market
- **Ready to use low level software drivers (Platform Support Layer)** for peripherals, smartcard and cryptographic software: T=0, T=1, RSA, DES, AES, EC,…
- **Worldwide application engineer team & customer dedicated Field Application Engineers.**
- **Regular customer trainings on hardware & software tools**, on-site trainings available on request.

Document References

- **Hardware Reference Manual**
- **Programmer's Reference Manual** with complete set of application notes and program examples
- **Production and Personalization Manual** for flash loading and production optimization
- **Chip qualification report**
- **Chip delivery specification** for wafer with chip-layout (die size, orientation, step size)
- **Module specification** containing description of package
- **Module qualification report**

Electrical Characteristics

- External clock frequency: 1 to 10 MHz
- Supply voltage range: 1.62 V to 5.5 V
- Temperature range: -25°C to +85°C
- ESD protection $\geq$ 6 kV (HBM)
- Max. sleep mode current (typical) < 100 µA in clock off mode

Supported Standard

- ISO/IEC 7816
- GSM 11.11, 11.12, 11.18
- ETSI TS 102 221
- ETSI TS 102 613 Release 7

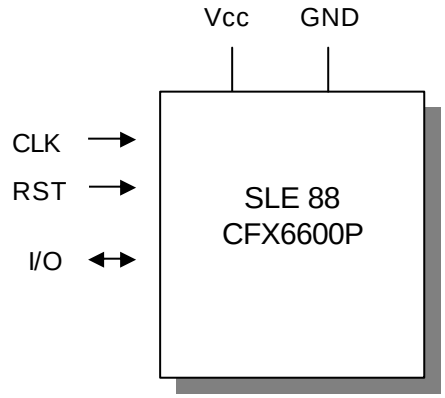
Ordering Information

Type	Package[1]	Voltage Range	Temperature Range	Frequency Range (ext. clock frequency)
SLE 88CFX6600P C	Die (sawn, unsawn)	1.62 V - 5.5 V	– 25°C to + 85°C	1 MHz - 10 MHz
SLE 88CFX6600P MXXX	M5.x MFCxxx			

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

Flash initialization/personalization available upon request.
For ordering information please contact your Infineon local sales representative.

Pin Description and Packaging



Pin symbol	Function
Vcc	Operating voltage
RST	Reset input
CLK	Processor clock input
GND	Ground
I/O	ISO7816-3 bi-directional data port

General Description

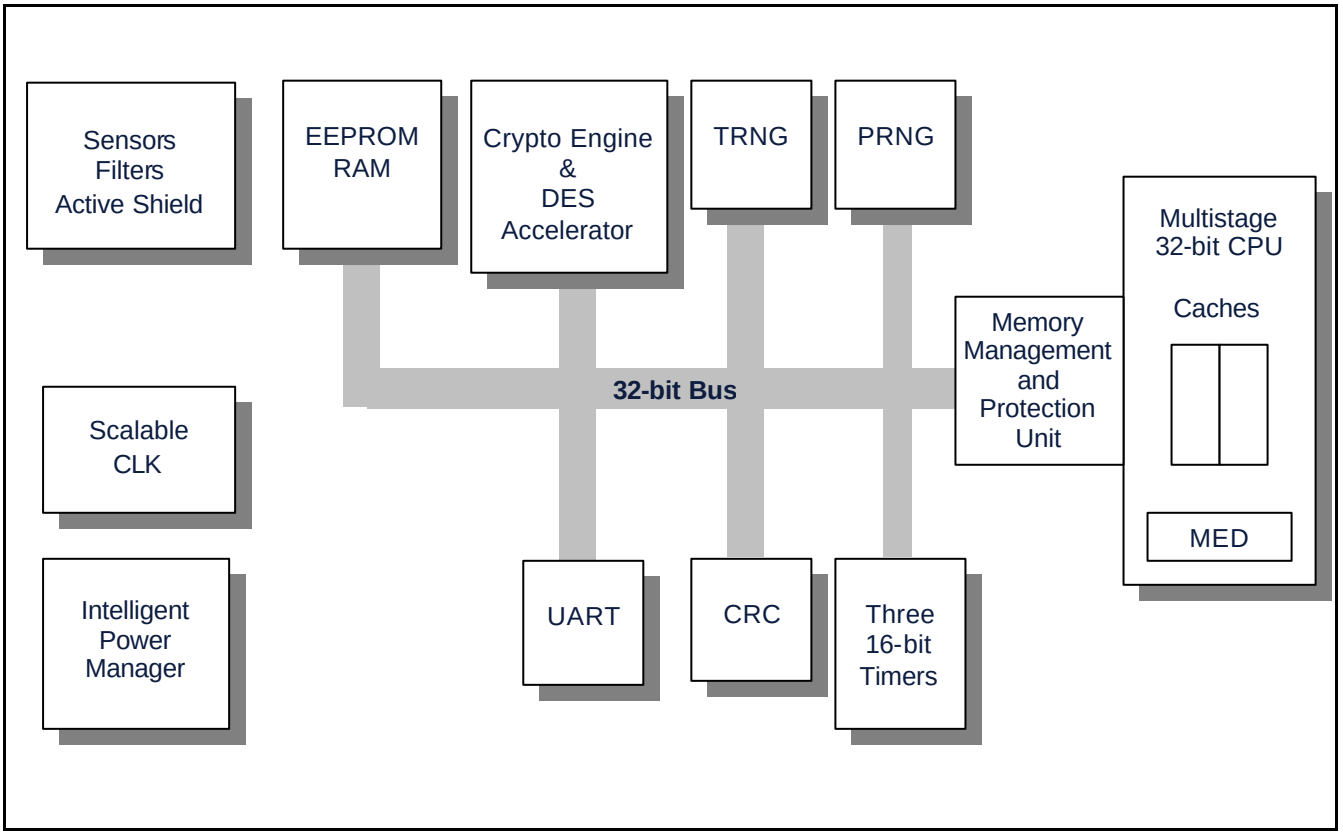
The SLE 88 products family is the **Infineon's state of the art 32-bit platform**, designed in cost optimized 130nm technology, with:

- **High Security** level enabling secure multi-application and multitasking
- **High Performance** for SIM/UICC applications with a fast internal frequency (33-66MHz)
- **High Quality EEPROM** with 500,000 cycles programming endurance
- **High Flexibility** with a freely configurable memory in code and data

The SLE 88CFX6600P brings a significant layer of security and convenience to mobile applications like digital signature and mobile TV. It offers as well an easy migration to the SLE 88CNFX6602PM dedicated for NFC (Near Field Communication) applications.

With its flash capability, it offers a decisive time-to-market advantage to card vendors and service providers in the launch of GSM/UICC applications.

Technical Description



The SLE 88 Family fully meets the requirements for **real multi-application operating systems**. 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.

The **High Performance** is ensured by the 32-bit RISC architecture that processes instructions and data 32-bit wise supplied by 2 dedicated caches. A very efficient context/application switching mechanism allows fast switching between multiple tasks.

An **Integral Security Concept**, based on the entire integration of security measures at each hardware and software design phase, has been used for the development of the SLE 88 Family.

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).

The architecture allows the **Linear Addressing of Large Memories** for a more convenient code implementation. 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. Program and data modules are organised as packages. Each package has a defined memory range of 16 Mbytes with dedicated access rights for memories and peripherals.

With the 0.13µm process, the SLE 88 Family offers large on-chip memories (ROM, EEPROM, RAM). The EEPROM space is the basis of **Infineon Technologies "Flash" Concept where the entire EEPROM is freely configurable in code and data sections**, and so can be used to store an Operating System, as well as application code and data. This customization provides added value to the system and the possibility to serve multiple projects with the same platform. **This concept offers the flexibility and convenience of Flash memory, but takes advantage of the EEPROM cell quality (timing, cycling and endurance)**.

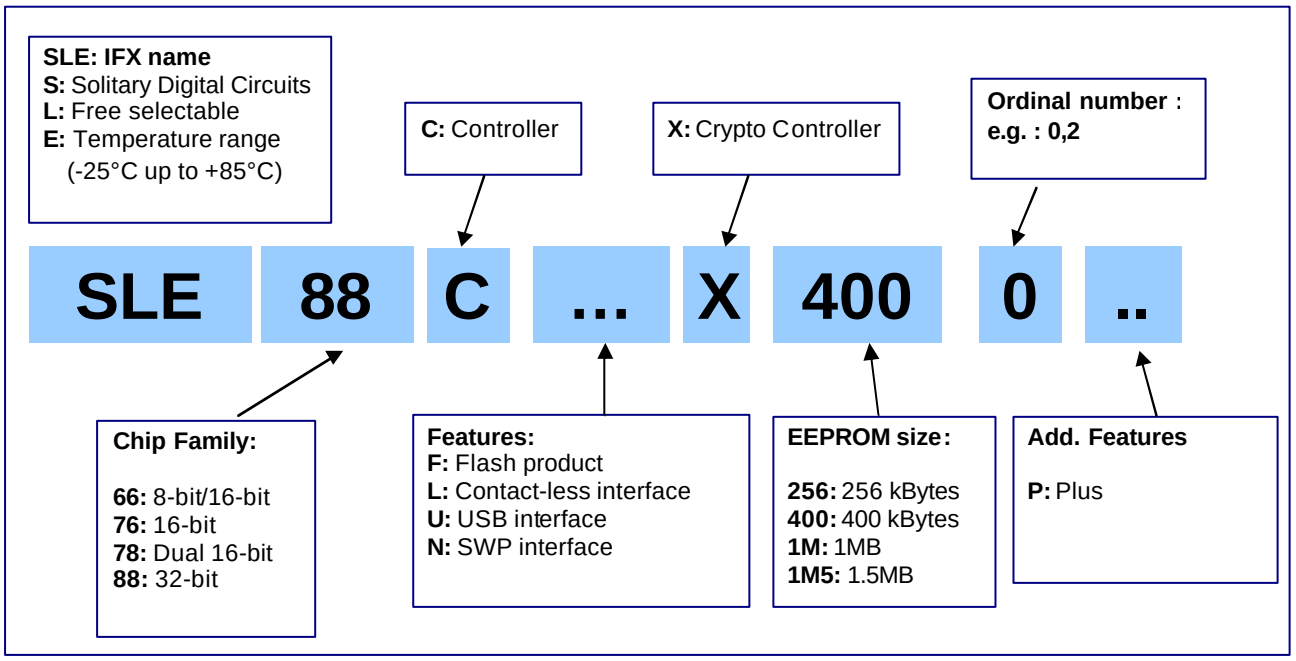
A number of powerful peripherals offer hardware support for time and code intensive operations. :

- **Crypto@1408** for all known public-key algorithms based on large integer modular arithmetic with configurable register lengths of up to 1408 bits.
- **DES Accelerator** for symmetric crypto operations based on DES and Triple DES
- **True Random Number Generator** (TRNG) to supply the CPU with true random numbers whose quality is tested according to AIS-31 strict evaluation guidelines
- **Pseudo Random Number Generator** (PRNG) for very fast generation of random numbers
- **Intelligent Power Manager** which automatically adjusts the internal frequency accordingly to the power classes A,B,C
- **Three 16-bit timers** for protocol implementation, event monitoring, etc…
- **CRC hardware module** for fast CRC calculations

Glossary

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 fast RAM memories integrated into the CPU (faster access than external RAM)
CRC	Cyclic Redundancy Check
CPU	Central Processing Unit
CMOS	Complementary Metal-Oxide Semiconductor (technology used to manufacture most of today's chips)
DES	Data Encryption Standard
EC	Elliptic Curves
EEPROM	Electrically Erasable Programmable Read-Only Memory (equivalent to NVM)
ESD	Electrostatic Discharge, release of static electricity that can damage a chip
ETSI	European Telecommunication Standards Institute
FPGA	Field Programmable Gate Array
GSM	Global System for Mobile Communication
HBM	Human Body Model
ISO/IEC	International Organization for Standardization/International Electrotechnical Commission
MED	Memory Encryption Decryption unit
MMU	Memory Management Unit
NVM	Non Volatile Memory
OS	Operating System
PRNG	Pseudo Random Number Generator
RAM	Random Access Memory
RISC	Reduced Instruction Set Computer
ROM	Read-Only Memory
RSA	Rivest, Shamir and Adleman, inventors of the RSA cryptosystem
T=0, T=1	Communication Protocols defined in ISO 7816 standard
TRNG	True Random Number Generator
UART	Universal Asynchronous Receiver/Transmitter
UICC	Universal Integrated Circuit Card

Sales code name



For ordering information please contact your Infineon local sales representative