Chip Card & Security

SLM 76CF3601P

360 kBytes E²PROM
8 kBytes RAM

16-bit ROM-less security controller optimized for
M2M applications
in 0.13 µm CMOS technology

Short Product Information January 2010

SLM76CF3201P Short Product Information	Ref.: SPI_SLM76CF3601P_1108
Revision History: Current Version 01.2010	
Previous Releases: 11.2008	
Page	

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

Published by Infineon Technologies AG, CCS
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.

16-bit security controller optimized for M2M applications with enhanced operating conditions in 0.13 µm CMOS technology, 8 kBytes RAM and 360 kBytes E²PROM

General Features

- 16-bit microcomputer in 0.13 µm CMOS technology with 24-bit linear addressing
- Highly efficient instruction set based on an 80251 type architecture
- Up to 16 Mbytes linear address space
- 68 bytes register file with 11 double word, 16 word and 16 byte registers
- **Defined migration path from SLE50PE products with minimized customer effort based on an adapted tool set**
- **SW compatible with SLE76P**
- Dedicated, 80251-based architecture implementation with an execution time faster than a standard 80251
- **360 kBytes E²PROM** with full E²PROM functionality and free partitioning between code and data
- **8 kBytes RAM**
- **1 kByte unified cache** for code and data
- **Symmetric Crypto Processor (SCP)** for triple-key, triple-DES and AES acceleration (128, 192 and 256-bit)
- **External Clock frequency 1 up to 10 MHz**
- **Internal Clock** with up to 33 MHz: Programmable internal frequency (PLL x1…x8 and free running mode.
- **Autamatically adjustable internal frequency according to available power or required performance**
  - Increased internal frequency for maximum performance
- Two 16-bit Autoreload Timers and Watch Dog Timer
- **Enhanced UART for handling serial interface** in accordance with ISO/IEC 7816 part 3 **supporting transmission protocols T=1 and T=0 (support of clock division factor of 8)**
- Improved CRC module with loadable initialization vector (developed according to ISO/IEC 3309 supporting CCIT v.41 & HDLC X25)
- Supply voltage range: 1.62 V to 5.5 V
- Support of current consumption limits
  < 10 mA @ 5.5 V
  < 6 mA @ 3.3 V
  < 4 mA @ 1.98 V
- Operating temperature range: -40 to + 105°C
- Storing temperature range: - 40° to +125°C
- ESD protection larger than 4 kV (HBM)

E²PROM Technology

- Typical programming time (erase & write) = 2.3 ms
- Fast personalization mode = 1 ms per page
- Flexible page mode for 1 to 128 bytes write/erase operation for the whole NVM size
- **Flash Loader concept**
  - High speed flash download for fast personalization (10s / 512k)
  - Flash upload service by Infineon (optional)

Additional features tailored for machine-to-machine (M2M) applications

- **Extended temperature range** -40 to +105°C
- Vibration Variable Frequency (VVF) according to JESD22-B103
- Temperature Humidity Bias (THB) according to JESD22-A101Humidity
- **Advanced E²PROM technology** with
  - Typical 500.000 write/erase cycles @ 85°C per page; max. 500,000 programming cycles @ 105°C per page; max.cycling of 16.5 million can be reached for 1 hot spot / sector
  - Typical data retention of 10 years @ 85°C; max. 10 years at 105°C

Memory Security

- Memory Management and Protection Unit (MMU)
  - Addressable memory up to 8 security level
  - Code execution from RAM possible
- 32 bits security area (PROM)
- Unique chip identification number for each chip
- MED – memory encryption/decryption device for RAM, ROM, and NVM in code or data areas

Document References

- Confidential Hardware and Programmer Reference Manual (see manual of SLE76/SLM76)
- 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

Development Tools Overview

- Software Development Kit, SDK 70 (based on the Keil PK251 kit)
- FPGA based emulator ET70
- Tool support for VQFN-8-1 package
- Worldwide application engineer team & customer dedicated Field Application Engineers
- Regular customer trainings on hardware & software tools
- On-site trainings available on request

Security features tailored for mobile communication applications

- Light sensors
- Special Function Register (SFR) encryption
- User mode Security Life Control (UmSLC)
- Pseudo Random Number Generator (PRNG)
- Interrupt and Peripheral Event Channel Controller (ITP)
  - Interrupt module for I/O interface and peripherals
  - Enabling fast data transfer through peripheral event channels (PEC)
- fast data transfer through peripheral event channels (PEC)
- Watchdog Timer (WDT) incl. check point register for runtime check
- Address and data scrambling of memories

Anti Snooping

- Basic countermeasures against side-channel attacks
- Dedicated smart card controller micro-architecture

Supported Standards

- ISO/IEC 7816
- GSM 11.11, 11.12, 11.18
- ETSI TS 102 221
- ETSI TS16949 automotive standard
- JESD22-A101
- JESD22-B103

Ordering Information

Type	Package	Voltage Range	Temperature Range	Frequency Range (ext. clock frequency)
SLM76CF3601P C	Die (sawn, unsawn)	1.62 V - 5.5 V	– 40°C to +105°C	1 MHz - 10 MHz
SLM76CF3601P MXXX	P-M2M5.1-8			
SLM76CF3601P VQFN-8-1	VQFN-8-1	1.62 V - 5.5 V		

Flash initialization/personalization available upon request.

For ordering information please refer to the Hardware Reference Manual and contact your sales representative.

VQFN-8-1 package description

VQFN-8-1 offers an optimized design, material and process enabling high performance operation

Temperature Range: -40° bis 105°C

Moisture sensitivity characterization:	MSL 3 with 260°C peak temperature
Temp / Humidity Bias:	85°C / 85% RH, 1000 hours
High temp storage:	150°C, 1000 hours
Temp cycle:	-55°C / +125°C, 1000 cycles
Autoclave	121°C, 100% RH, 96h

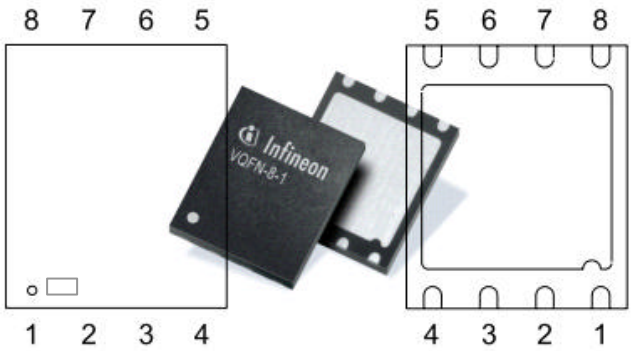
Process Highlights:

Die Thickness:	.25 ± .05 nominal
Plating:	NiPdAu
Marking:	Laser

Standard Materials:

Leadframe:	Cu roughened µPPF
Die attach:	AMK-06 Epoxy
Wire:	Au
Mold compound:	Nitto 7470-LA

Pin Description & Module



VQFN-8-1 Surface Mount package

BD = Bonding option

◦ = Index Marking

▭ = Bonding Index for VQFN 8a Pin Out version 2

Pin Out version 1
VQFN 8 (BD1-2):

Pin #01 = VSS
Pin #02 = I/O
Pin #06 = CLK
Pin #07 = RST
Pin #08 = VDD

Pin Out version 2
VQFN 8a (BD1-3):

Pin #01 = VSS
Pin #03 = I/O
Pin #06 = CLK
Pin #07 = RST
Pin #08 = VDD

P-M2M5.1-8-1 (molded chip card module)

Pin Out version
Molded chip card module

Pin #01 = VSS
Pin #03 = I/O
Pin #06 = CLK
Pin #07 = RST
Pin #08 = VDD

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 SLM76CF3601P is a member of the SLM76P-series of Infineon Technologies optimized for machine-to-machine (M2M) applications. This security controller is manufactured in advanced 0.13 µm CMOS technology. It has a defined migration path from existing SLE50CxxxPE products with minimized customer effort to migrate the OS and is based on the same tool set. SLM76P-series is compatible with SLE76P.

Specially optimized for M2M applications, operating at high temperature and offering EEPROM cycling resistance at high temperature

ROM-less concept: The unique NVM combines the advantages of a high speed code Flash with the flexibility and reliability of a true E²PROM with regard to bytewise addressable pages and data retention.

Performance

The internal clock frequency can be adjusted to a level of up to 33 MHz either as a multiple of 1 to 8 of the external frequency or independent of the clock rate of the terminal with the help of the internal clock. It is automatically adjustable according to either available given power requirements limitor delivering best performance required performance:without violating power constrains.

Memory

The SLM76CF3601P offers 8 kBytes RAM and 360 kBytes E²PROM. with full E²PROM functionality and free partitioning between code and data thus allow to include SIM Application Toolkit, Wireless Application Protocol (WAP), WML-Browser and JavaCard API implementations into the NVM.

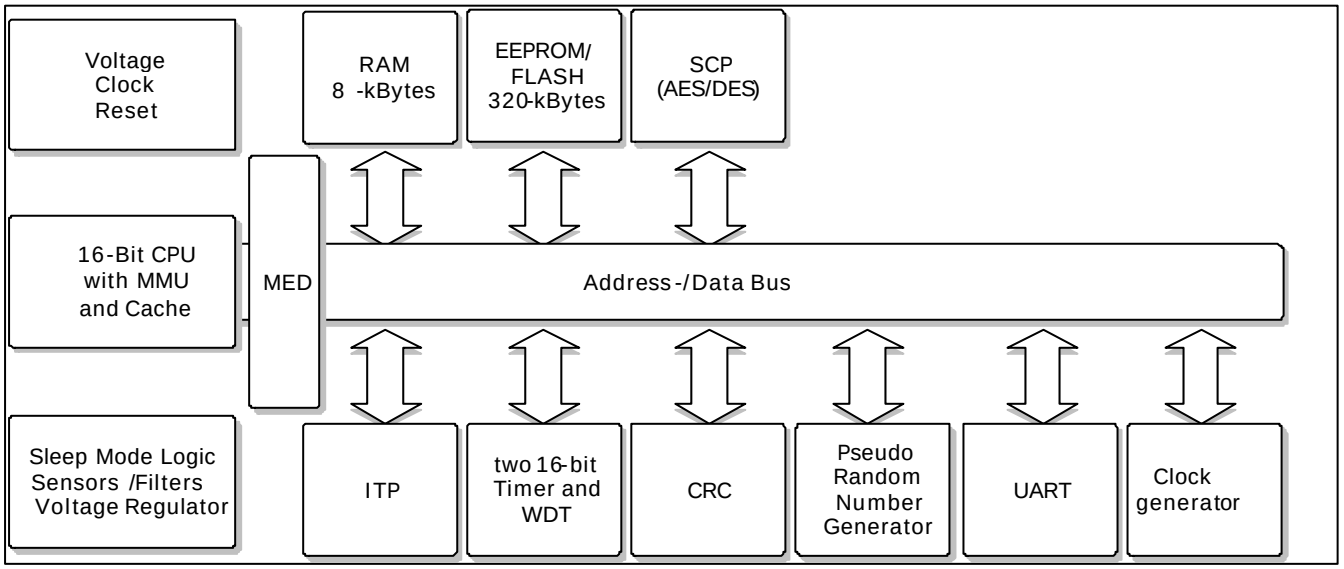


Figure 1: Block Diagram SLM76CF3601P

The new platform is designed to address up to 16 Mbytes of memory.

Security

The set of security features has been tailored to fit the requirements of M2M applications 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) / Fault Induction Attacks.
- A customer specific transport key combined with a unique loader concept secures the logistic flow until card issuing.

Peripherals

The SCP (Symmetric Crypto Processor) module supports symmetrical crypto algorithms according to the Data Encryption Standard (DES) in the Electronic Code Book Mode, as well as Cipher Block Chaining, while the AES (Advanced Encryption Standard) component of the SCP module performs AES-compliant operations for three different key lengths.

The Interrupt and Peripheral Event Channel Controller (ITP) can process interrupt requests from different sources to run an interrupt service routine (ISR). Data can be directly transferred between memory locations with a minimum of CPU activity for fast interaction with peripherals using so-called Peripheral Event Channels (PECs). The channels can be assigned individually to peripherals or chained together to enable continuous transfer without handover delay between the channels.

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.

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 and a clock division factor of 8. 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 pseudo random number generator (PRNG) is able to supply random numbers.

The watchdog timer (WDT) is a circuit that monitors controller operation by automatically initiating a security reset if a specified period without an adequate response elapses after occurrence of a hardware or software irregularity.

In conclusion, the SLM76CF3601P fulfills all requirements of today's M2M smart card applications. In addition, it offers a powerful platform for multi application cards based on Java.

The SLM76CF3601P integrates outstanding memory sizes and peripherals in combination with enhanced performance and optimized power consumption on a minimized die size, together with resistance to extreme conditions, such as high temperature, EEPROM cycling at high temperature, vibration or humidity, which are characteristics in M2M applications.

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
ETSI	European Telecommunication Standards Institute
FIFO	First In, First Out
FPGA	Field Programmable Gate Array
GND	Ground
GSM	Global System for Mobile Communication
HBM	Human Body Model
ISO/IEC	International Organization for Standardization/International Electrotechnical Commission
ITP	Interrupt and Peripheral event channel controller
MED	Memory Encryption Decryption unit
MMU	Memory Management Unit
NVM	Non Volatile Memory
OS	Operating System
OTP	One Time Programmable
PEC	Peripheral Event Channel
PROM	Programmable Read-Only Memory
PRNG	Pseudo Random Number Generator
RAM	Random Access Memory
RMS	Resource Management System
ROM	Read-Only Memory
RST	Reset
SCP	Symmetric Crypto Processor
SDK CC	Software Development Kit Chip Card
T=0, T=1	Communication Protocols defined in ISO 7816 standard
UART	Universal Asynchronous Receiver/Transmitter
Vcc	External Voltage (common-collector voltage)
PLL	Phase-Locked Loop
WDT	Watch Dog Timer

Sales code name