SLD 9670 X

Bayon

Infosys
we encrypt networks ≡ worldwide

Security & Chip Card ICs

Infineon
technologies

Never stop thinking.

SLD 9670 X Prel. Short Product Information	
This document contains preliminary information on a product under development. Details are subject to change without notice.	
Revision History: Current Version 2000-11-09	
Previous releases:	
Page	Subjects (changed since last revision)

Important:	Further information is confidential and on request. Please contact Infineon Technologies AG in Munich, Germany Security and Chip Card ICs Phone +49 89 234 80000, Fax +49 89 234-81000 E-Mail: security.chipcard.ics@infineon.com

Edition 2000-11-09

Published by Infineon Technologies AG,
St.-Martin-Strasse 53,
D-81541 München, Germany

and

Computer Elektronik Infosys GmbH
Am Kuemmerling 45, D-55294 Bodenheim

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.

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.

Features

- Standard PCI master/target interface (32 Bit/33 MHz) according to 'PCI Local Bus Specification, V2.2'
- PCI power management capabilities according to 'PCI Bus Power Management Interface Specification, V1.1' (wake up from states D1 and D2) and 'PCI Mobile Design Guide, V1.1'
- Integrated security controller as on-chip processor (OCP), providing 56k ROM, 88k RAM and 32k EEPROM
- DES CryptEngine (single and triple DES, MAC), 423 Mbit/s ECB/CBC provides high speed, high volume data encryption
- Advanced crypto engine (ACE) for public key algorithms (e.g. RSA) and elliptic curves provides highest flexibility for secure protocol algorithms making use of hardware security
- Hardware solution for hash value calculations (algorithms MD5 and SHA-1)
- Extended key length and sophisticated key management, automatic key erasure when device is tampered with
- Nonvolatile key storage (EEPROM and battery powered RAM)
- Scalable security profile
- Silicon security (Active Shield, sensors)
- Two security inputs (tamper, pull-out detect)
- Battery powered real time clock (RTC)
- Two built-in serial interfaces (chip card terminals according to ISO7816 or standard RS232)
- General purpose I/O port
- High speed local security bus SFPI (Secure FPI) based on SIEMENS 'Flexible Peripheral Interconnect' bus protocol for high speed internal data transfer
- Core supply voltage 2.2 V
- Overall power consumption 500 mW
- Temperature range: -25 to +70°C
- ESD protection larger than 2 kV HBM

PCI-Target

- Zero wait state read/write operation
- Target FIFO depth 8 DWORDs in both directions
- Support of prefetchable and non-prefetchable read
- Support of posted write
- Fast back-to-back operation
- Endian conversion (byte swapping 16/32)
- Memory and I/O space available
- SPI EEPROM interface supporting 8/16/24 Bit addressing modes for configuration space backup and BIOS extension (up to 128 kB)

PCI-Master

- Zero wait state read/write operation
- Master FIFO depth 64 DWORDs in both directions
- Endian conversion (byte swapping 16/32/64)
- Memory and I/O space available
- DMA capability to host memory

DES CryptEngine

- High-speed cryptographic operations using DES and DES-like loadable algorithms
- Loadable S-boxes for DES-like algorithms
- All known DES operation modes:
  - ECB (Electronic Code Book)
  - CBC (Cipher Block Chaining)

Features (cont'd)

  - CFB (Cipher Feedback, 64/8/1 bit blocks)
  - OFB (Output Feedback, 64/8/1 bit blocks)
- KSG (Key Stream Generator)
- MAC Generation using CBC (Message Authentication Code)

On-Chip Processor (OCP)

- Infineon's security architecture
- 16-bit microcontroller in deep sub-micron CMOS technology
- Instruction set opcode compatible with standard 8051 controller
- Enhanced 16-bit arithmetic
- Additional powerful instructions optimized for chip card applications
- Dedicated, non-standard architecture with execution time six times faster than standard 8051 controller at same clock
- 56k user ROM for application programs
- max. 2k reserved ROM for Resource Management System (RMS) with intelligent EEPROM write/erase routines
- 32k EEPROM
- 88k XRAM (battery powered), 256 bytes IRAM
- Memory Management Unit (MMU)
- DES and EC2 accelerator (GF 2n), used e.g. for key management purposes
- Advanced Crypto Engine (ACE)
- CRC Module
- Interrupt Module (16 sources)
- two 16-bit autoreload timers
- Power saving sleep mode
- programmable PLL (up to 15 MHz)
- External clock frequency 1.5 to 7 MHz (nominal 3.57 MHz)
- Two Terminal UARTs for handling serial interface in accordance with ISO/IEC 7816 supporting transmission protocols T=0 and T=1

EEPROM

- Reading, erasing and writing byte by byte
- Flexible page mode for 1 to 64 bytes write/erase operation
- Write time < 4.5 ms
- Programming time independent of clock frequency
- Minimum of 500.000 write/erase cycles at 25°C
- Data retention for a minimum of 10 years
- EEPROM programming voltage generated on chip

MMU

- Addressable memory up to 1 Mbyte
- Separates OS (system) and application (user)
- System routines called by traps
- OS can restrict access to peripherals in application mode
- Multi application enabled
- Code execution from XRAM possible

Security Features

- Low and high voltage sensors
- Low-frequency sensor
- High-frequency filter
- True random number generator (RNG)
- Internal power-on-reset
- 16 bytes security PROM, hardware protected
- Unique chip identification number for each chip
- Security optimized layout

Features (cont'd)

- Active shield
- Secure local bus SFPI

Package

- P-TQFP-144-2

Typical Applications

- User authentication (Chip card + PIN-code)
- User profiles (access rights, working time)
- Data security (disk encryption)
- Secure Networking in private and public environment (Internet, e-mail; TCP-IP, SSL)
- Banking Applications (Money Exchange)
- Electronic Commerce
- Governmental Applications

Support

- HW-& SW-Tools (Emulator, Simulator)
- Application Notes

General Description

The Bayon is a high performance crypto controller chip for PCI-based computer systems.

Its DES CryptEngine performs high-speed cryptographic operations using DES and DES-like[1)] loadable algorithms, MAC calculation, KSG (key stream generator). The DES CryptEngine is intended to be used for mass encryption which needs highest data throughput.

Sophisticated key management, extended keys with lengths up to 3x112 Bit keys in triple-DES operation and the ultra DES kernel performance of 423 Mbit/s (single-DES, ECB/CBC mode) and 141 Mbit/s (triple-DES, ECB/CBC mode) provide highest data rates in all encryption modes.

A fast random number generator (FRNG) has been included which provides true random numbers in all conditions. This can be used for fast session key generation in networking applications.

Hash values according to the algorithms MD5 and SHA-1 can be calculated using the special hash hardware of the CryptEngine.

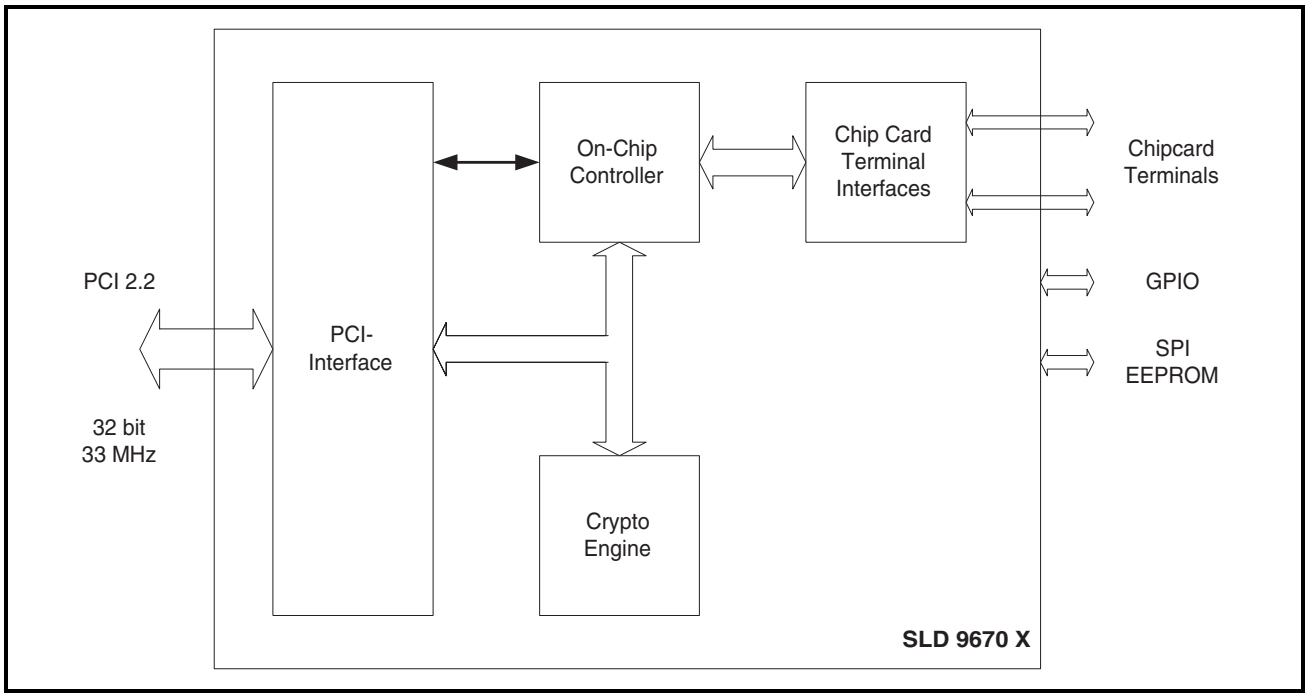

Figure 1 Block Diagram of the SLD 9670X (Bayon)

Data transfers between the DES CryptEngine and the PCI master/target interface are executed via a dedicated, FIFO supported 32 bit interface to assure highest communication speed for DES or triple-DES based mass data encryption.

1) The term 'DES' used only in case of S-Box contents referring to published 'Data Encryption Standard (DES)'. Otherwise, DES-'like' algorithms are executed.

The integrated 32 bit/33 MHz PCI interface conforms to the 'PCI Local Bus Specification, V2.2' and provides zero wait state read/write operations as well as PCI power management capabilities according to the 'PCI Bus Power Management Interface Specification, V1.1' (wake-up from D1/D2) and 'PCI Mobile Design Guide V1.1'.

The configuration and the key management for data encryption is controlled by the embedded on-chip controller which is based on Infineon's high end security controller family in advanced deep sub-micron CMOS technology. The CPU provides the high efficiency of the 8051 instruction set extended by additional powerful instructions together with enhanced performance, memory sizes and security features. The internal clock frequency can be adjusted up to 15 MHz independent of the clock rate of the terminal by using the integrated PLL.

The controller offers 56 kByte of User-ROM, 256 bytes internal RAM, 88 kByte XRAM and 32 kByte EEPROM. The memory management unit (MMU) allows a secure separation of the operating system and the applications. With its help, multi-applications are also possible.

With its powerful internal peripherals, the embedded controller completes the capabilities of the DES CryptEngine with asymmetrical cryptographic algorithms, local DES and EC2 accelerator, CRC module and two serial interfaces which can be configured as terminal UARTs. The DES kernel local to the OCP is used e.g. for key management purposes which do not need the high performance of the DES module integrated in the DES CryptEngine.

The CRC module allows the easy generation of checksums according to ISO/IEC 3309 (16-bit CRC). To minimize the overall power consumption, the controller offers a sleep mode.

Each of the two independent serial interfaces can be used as chip card terminal according to ISO/IEC 7816 with card detection and built-in ISO startup/stop sequence logic or as a full-duplex RS232-interface with hardware handshake (DSR, DTR). Speeds of up to 223 kbit/s can be handled. The interfaces operate in 5V or 3.3 V CMOS environments. When configured as Terminal-UARTs, 5V/10mA (min. 4.5V/10mA @ VDD5 = 4.75V) are directly supplied. Furthermore, they support the half-duplex transmission protocols T=0 and T=1 according to ISO/IEC 7816-3. All relevant transmission parameters can be adjusted by software, 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, e.g. I^2C routines. Two pins can be configured alternatively as push-pull or open-drain drivers.

The advanced crypto engine is equipped with its own RAM of 700 bytes and supports all public-key algorithms known today which are based on large integer modular arithmetic. It allows fast and efficient calculation of e.g. RSA operations with key lengths of up to 2048 bit.

The DES accelerator of the OCP consists of two modules. The DES module supports symmetrical cryptographic algorithms according to the Data Encryption Standard in the electronic code book mode. The EC2 module accelerates the multiplication in GF(2n) and therefore the operations for elliptic curve cryptography.

The random number generator (RNG) is able to supply the controller with true random numbers under all conditions.

To connect the powerful modules of the Bayon (DES CryptEngine, PCI-interface and on-chip processor), a 32-Bit local bus with enhanced security features is used (SFPI - 'Secure Flexible Peripheral Interconnect'). The bus protocol is based on SIEMENS 'Flexible Peripheral Interconnect' bus system. Furthermore, an X-box is used to exchange commands, parameters and status information between the PCI-interface and the on-chip processor. So the OCP can be invoked to change keys or to encrypt data, using a special algorithm, by addressing commands via PCI.

As an important measure, the chip provides a new and enhanced level of on-chip security features.

In conclusion, the Bayon fulfills the requirements of a secured computer platform, providing data security (encrypted harddisk, floppy disk), user authentication (chipcard and PIN), user profile handling (access rights, working time) and last, but not least, secure networking in private and public environment (Internet, e-mail; ISDN, TCP-IP, SSL, SHTTP). It is compatible to the PC-2000 specification as well.

Glossary

ACE	Advanced Crypto Engine
CBC	Cipher Block Chaining
CLL	Contact-Less Logic
CFB	Cipher Feedback
CRC	Cyclic Redundancy Check
DES	Data Encryption Standard
EC2	Elliptic Curves
EPP	Enhanced Parallel Port
FIFO	First In First Out
GF	Galois Field
LPC	Low Pin Count Interface (Intel)
MED	Memory Encryption Device
MMU	Memory Management Unit
OCP	On Chip Processor
OFB	Output Feedback
OS	Operating System
PLL	Phase Locked Loop
RMS	Resource Management System
RNG	Random Number Generator
RSA	Rivest Shamir Adelman, Asymmetric crypto algorithm