Features

General

- Dual secureAVR® Master and Secure Cores
- High-performance, Low-power secureAVR RISC Architectures
  - 135 Powerful Instructions (Most Executed in a Single Clock Cycle)
- Total isolation between cores
- Secure Inter-Core Communication
- Low Power Idle Mode
- Bond Pad Locations Conforming to ISO 7816-2
- ESD Protection to ± 4000V on ISO pins and ± 2000V on Flash Interface Pins
- Operating Ranges: Class AB (2.7 to 5.5V) or Class A only (4.5 to 5.5V) depending on customer option
- Compliant with EMV 2000 Specifications, PC Industry Compatible
- Available in Wafers, Modules, and Industry-standard Packages

Memory

- Master Core
  - 128K Bytes of ROM Program Memory
  - 36K Bytes of EEPROM, Including 128 OTP Bytes and 384-byte Bit-addressable Bytes
    - * 1 to 128-byte Program / Erase
    - * 2ms Program / 2ms Erase
    - * Typically 500,000 Write/Erase Cycles at a Temperature of 25°C
    - * 10 Years Data Retention
    - * EEPROM Erase only mode
    - * Write EEPROM with or without autoerase
  - 6K bytes RAM Memory
- Secure Core
  - 64K Bytes of ROM Program Memory including 32K bytes of ROM with specific access
  - 18K Bytes of EEPROM, Including 64 OTP Bytes and 192-byte Bit-addressable Bytes
    - * 1 to 64-byte Program / Erase
    - * 2ms Program / 2ms Erase
    - * Typically 500,000 Write/Erase Cycles at a Temperature of 25°C
    - * 10 Years Data Retention
    - * EEPROM Erase only mode
    - * Write EEPROM with or without autoerase
  - 6K bytes RAM Memory (4K bytes of secureAVR RAM, 2K bytes of AdvX™ RAM, shared with the secureAVR core)
- Optional 1 to 8 Mbit Flash Memory

Secure Dual Core Microcontroller AT90SDC10x

Summary Preliminary

6568BS–SMS–11/09

Note: This is a summary document. A complete document will be available under NDA. For more information, please contact your local Atmel sales office.

Peripherals

- One I/O Port
- One ISO 7816 Controller
  - Up to 625 Kbps at 5 MHz
  - Compliant with T=0 and T=1 Protocols
- Serial Peripheral Interface (SPI) controller (up to 15 MBps) with Flash power management.
- Programmable Internal Oscillator (Up to 30 MHz for AdvX and 30 Mhz for both CPU Clocks)
- Two 16-bit Timers in Master Core and one 16-bit Timer in Secure Core
- Random Number Generators: PRNG on Master Core and AIS31 TRNG on Secure Core
- 2-level Interrupt Controllers
- Hardware DES and Triple DES DPA/DEMA Resistant
- Hardware AES DPA/DEMA Resistant
- Checksum Accelerators
- Code Signature Modules
- CRC16 & 32 Engines (Compliant with ISO/IEC 3309)
- 32-Bit Cryptographic Accelerator (AdvX for Public Key Operations)
  - RSA, DSA, ECC, Diffie-Hellman

Security

- Dedicated Hardware for Protection Against SPA/DPA/SEMA/DEMA Attacks
- Advanced Protection Against Physical Attack, Including Active Shield, EPO, CStack Checker, Slope Detector, Parity Errors
- Environmental Protection Systems
- Voltage Monitor
- Frequency Monitor
- Temperature Monitor
- Light Protection
- Secure Memory Management/Access Protection (Supervisor Mode)

Certification targeted

- CC EAL5+ (PPSSVG - BSI 0002)

Development Tools

- Voyager Emulation Platform (ATV5) to Support Software Development
- IAR Embedded Workbench® V4.30 Debugger or Atmel's AVR Studio® Version 4.07 or Above
- Software Libraries and Application Notes

Ordering informations

Part Number	Master Core			Secure Core			FLASH	Voltage	Available
	ROM	EEPROM	RAM	ROM	EEPROM	RAM			
AT90SDC100	128K	36K	6K	64K	18K	6K	N/A	2.7V-5.5V	Now
AT90SDC101	128K	36K	6K	64K	18K	6K	1 MBits	2.7V-5.5V	Q2 2010
AT90SDC102	128K	36K	6K	64K	18K	6K	2 MBits	2.7V-5.5V	Q2 2010
AT90SDC104	128K	36K	6K	64K	18K	6K	4 MBits	2.7V-5.5V	Q1 2010
AT90SDC108	128K	36K	6K	64K	18K	6K	8 MBits	2.7V-5.5V	Q3 2010

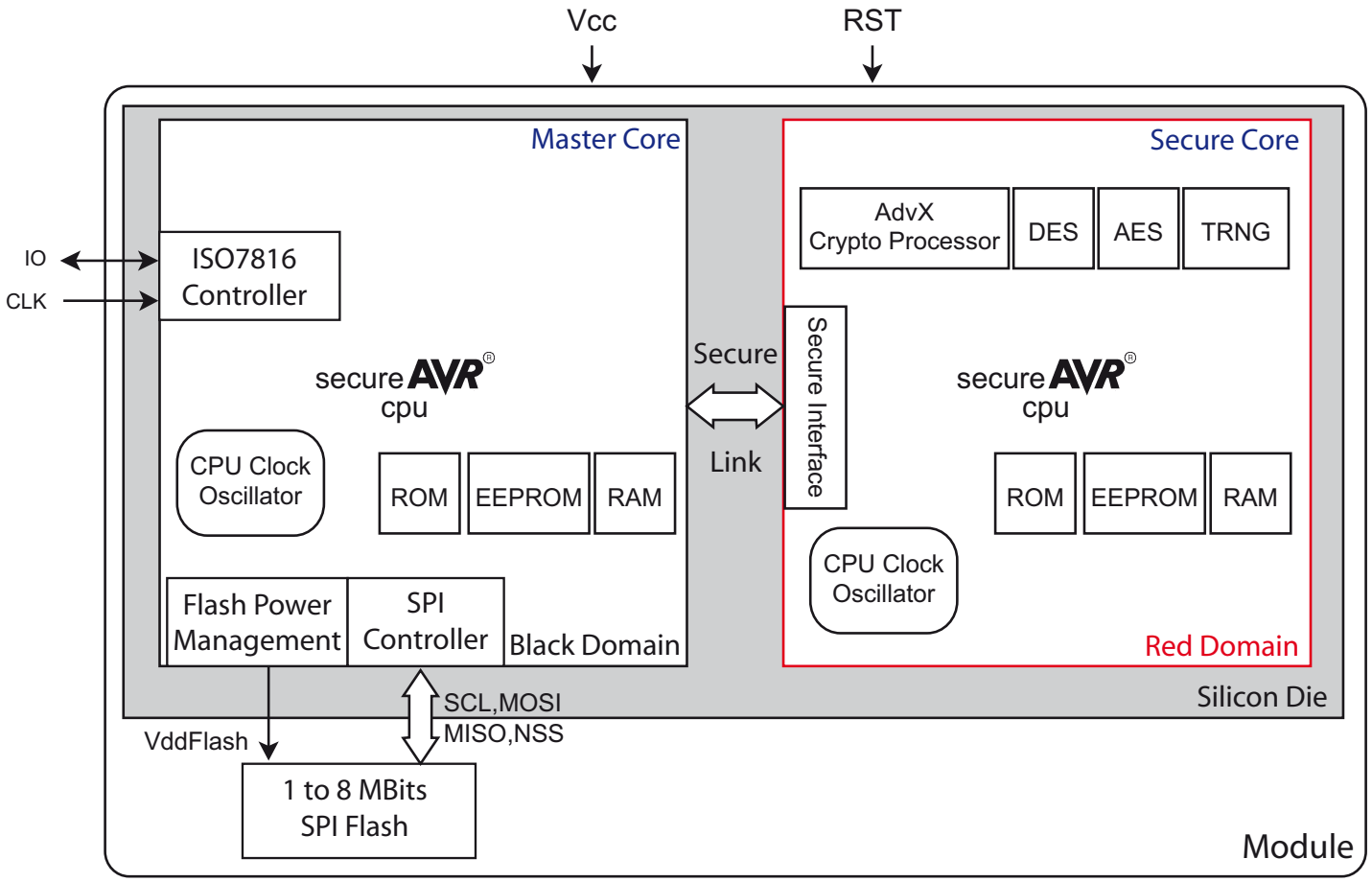
Description

The AT90SDC100 is a low-power, high-performance, microcontroller that contains 2 physical domains, the black domain and the red domain. Each domain features one independant 8/16-bit core running concurrently to each other. These cores, namely Master Core and Secure Core contains ROM program memory, EEPROM memory and RAM memory based on the SecureAVR enhanced RISC architecture.

By executing powerful instructions in a single clock cycle, each core achieves throughputs close to 1 MIPS per MHz. Its Harvard architecture includes 32 general-purpose working registers directly connected to the ALU, allowing two independent registers to be accessed in one single instruction executed in one clock cycle.

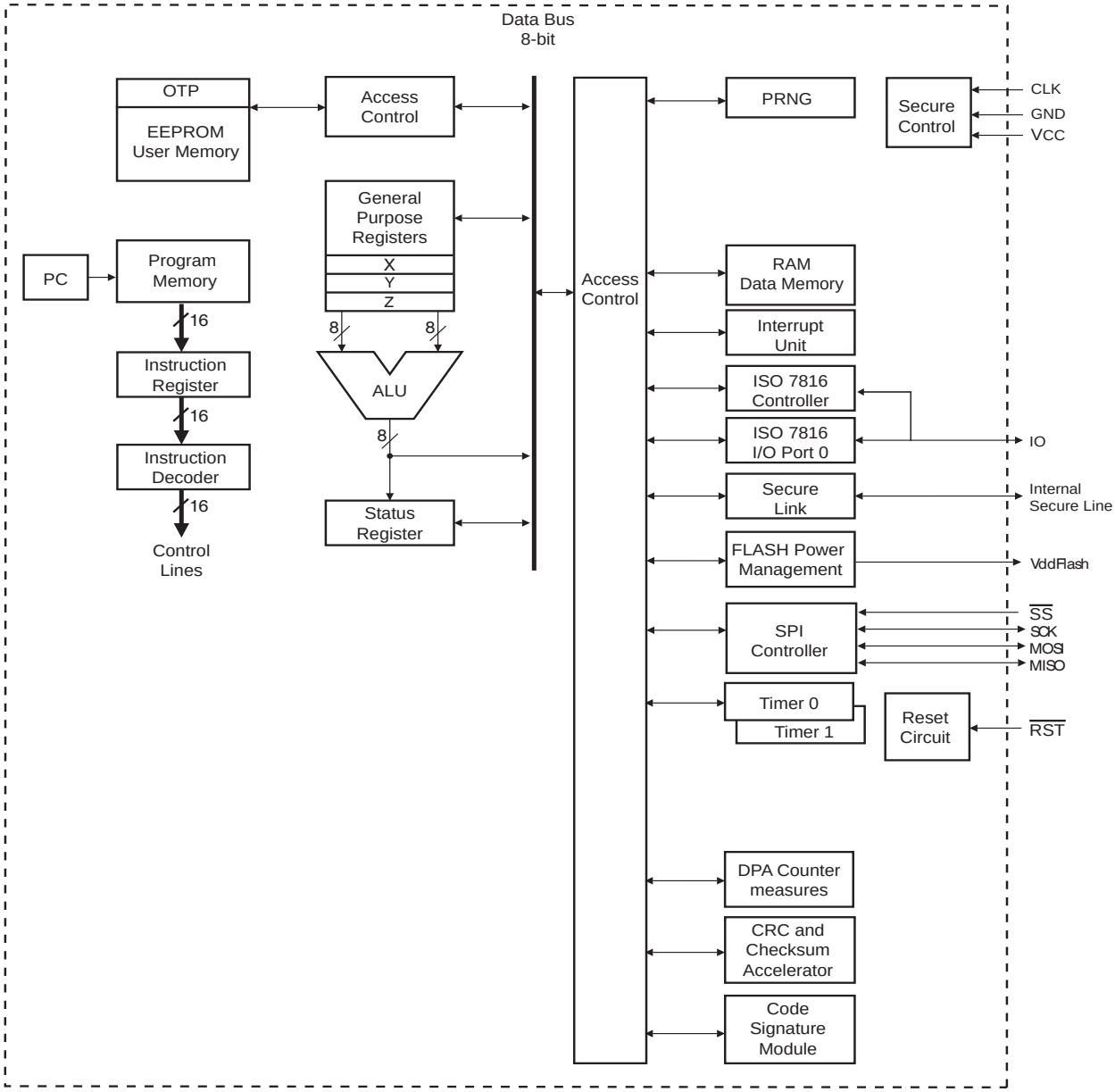
In order to prevent sensitive data leakage, each core can only communicate to each other using a Secure Link where only certified data can move from the Red Domain to the Black.

Figure 1 Chip Overview



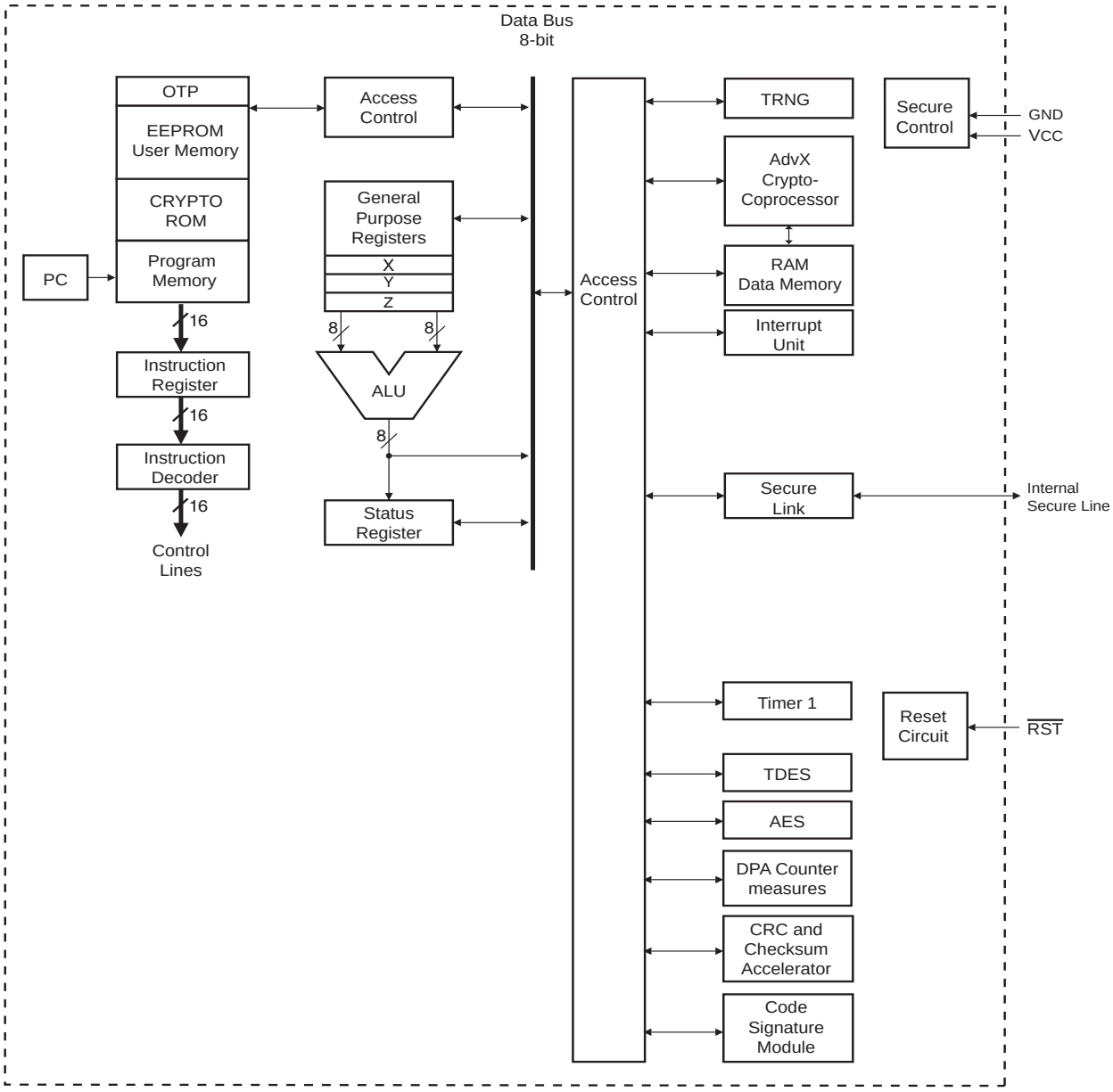
The Master core has direct access to the external world through the ISO controller. It also controls a SPI interface along with the appropriate power management to drive an external flash memory for mass storage. Alternatively, when used as a Slave, the SPI interface may also serve as an extra communication link.

Figure 2 Block diagram of the Master Core



The Secure Core is completely embedded in the device with no connection to the outside world. In addition to secure protection of data, it features all cryptographic peripherals for AES, TDES and RSA computation and Elliptic Curves to perform sensitive data management.

Figure 3 Block diagram of the Secure Core



Headquarters

Atmel Corporation
2325 Orchard Parkway
San Jose, CA 95131
USA
Tel: 1(408) 441-0311
Fax: 1(408) 487-2600

International

Atmel Asia
Unit 01-05 & 16, 19/F
BEA Tower, Millennium City 5
418 Kwun Tong Road
Kwun Tong, Kowloon
Hong Kong
Tel: (852) 2245-6100
Fax: (852) 2722-1369

Atmel Europe
Le Krebs
8, Rue Jean-Pierre Timbaud
BP 309
78054 Saint-Quentin-en-
Yvelines Cedex
France
Tel: (33) 1-30-60-70-00
Fax: (33) 1-30-60-71-11

Atmel Japan
9F, Tonetsu Shinkawa Bldg.
1-24-8 Shinkawa
Chuo-ku, Tokyo 104-0033
Japan
Tel: (81) 3-3523-3551
Fax: (81) 3-3523-7581

Product Contact

Web Site
www.atmel.com

Technical Support
at90sc@atmel.com

Sales Contact
www.atmel.com/contacts

Literature Requests
www.atmel.com/literature