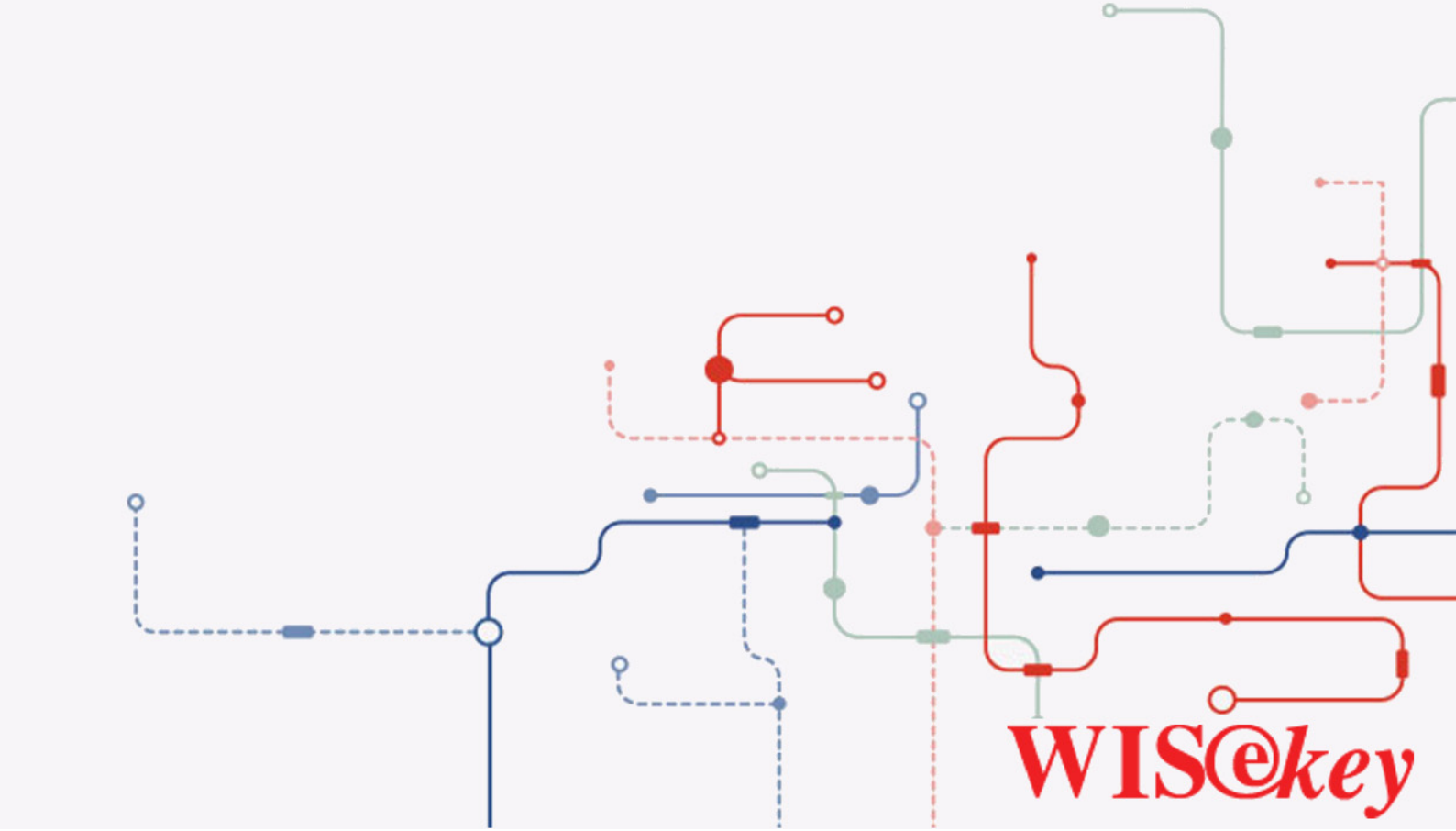
AT90SDC10X

Summary Datasheet



Features

General

- twincore™ Secure Dual Core Architecture
  - 135 Powerful Instructions (Most Executed in a Single Clock Cycle)
- Total isolation between Master & Secure 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

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)

Memory

- **Master Core**
  - 128K Bytes of ROM Program Memory
  - 36K Bytes of EEPROM , Including 128 OTP Bytes and 384 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 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 CPU RAM, 2K bytes of Ad-X™ RAM, shared with the CPU core)

- **Optional 1 to 8 Mbit Flash Memory**

Peripherals

- One I/O Port
- One ISO 7816 Controller
  - Up to 625 Kbps at 5 MHz
  - Compliant with T=0 and T=1 Protocols
- Four General Purpose I/O Ports
- Serial Peripheral Interface (SPI) controller (up to 15 MBps) with Flash power management.
- Programmable Internal Oscillator (Up to 30 MHz for Ad-X and 30 Mhz for both CPU Clocks)
- Two 16-bit Timers in Master Core and one 16-bit Timer in Secure Core

6578ES – 28Sep16

- 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 (Ad-X for Public Key Operations)
  - RSA, DSA, ECC, Diffie-Hellman

Certification Tageted

- CC EAL5+ (PPSSVG - BSI 0002)

Development Tools

- Voyager Emulation Platform (ATV4) to Support Software Development
- IAR Embedded Workbench® V4.30 Debugger or Above

Software Libraries and Application Notes

Ordering Information

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	TBD
AT90SDC102	128K	36K	6K	64K	18K	6K	2 MBits	2.7V-5.5V	TBD
AT90SDC104	128K	36K	6K	64K	18K	6K	4 MBits	2.7V-5.5V	Now
AT90SDC108	128K	36K	6K	64K	18K	6K	8 MBits	2.7V-5.5V	TBD

6578ES – 28Sep16

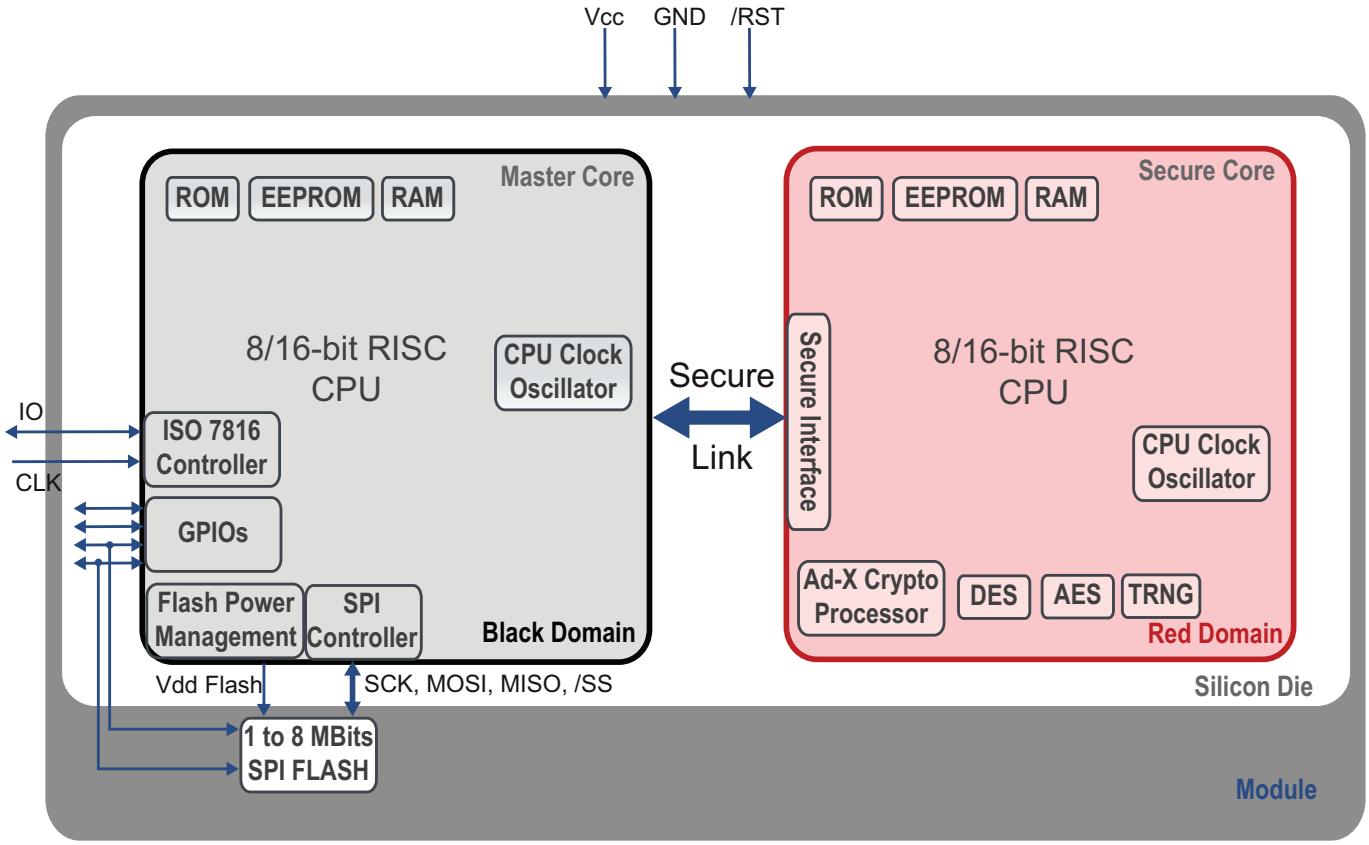
Description

The AT90SDC10X is a low-power, high-performance, microcontroller that contains 2 physical domains, the Black Domain and the Red Domain. Each domain features one 8/16-bit core running independantly from the other. These cores, namely Master Core and Secure Core contain ROM program memory, EEPROM memory and RAM memory based on the 8/16-bit enhanced RISC architecture.

By executing powerful instructions in a single clock cycle, each core achieves throughputs close to 1 MIPS per MHz. The core 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 with the other using a Secure Link where only certified data can move from the Red Domain to the Black Domain.

Figure 1 AT90SDC10X Chip Overview

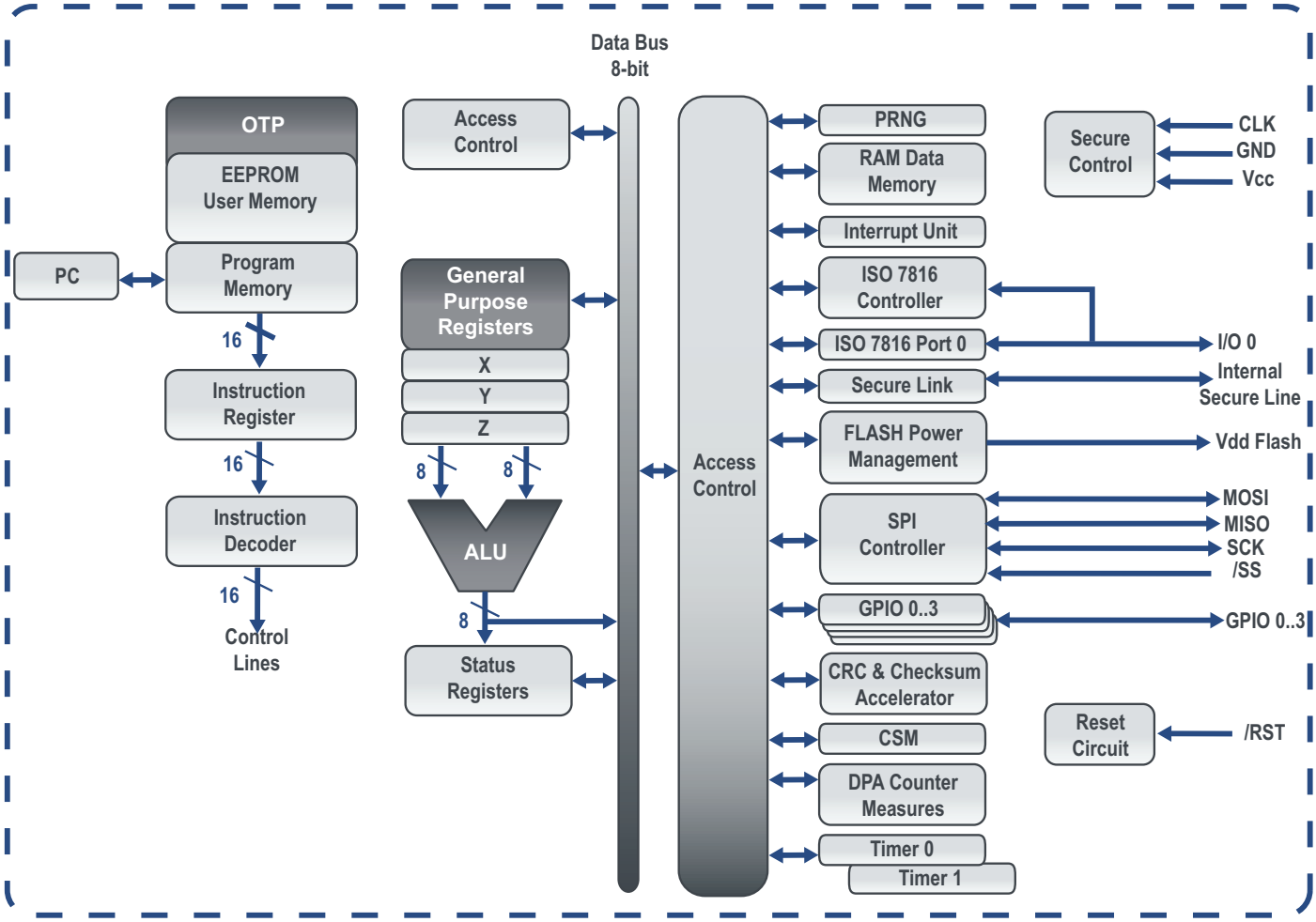


6578ES – 28Sep16

Master Core

The Master core has direct access to the external world through the ISO controller. It also controls an 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.

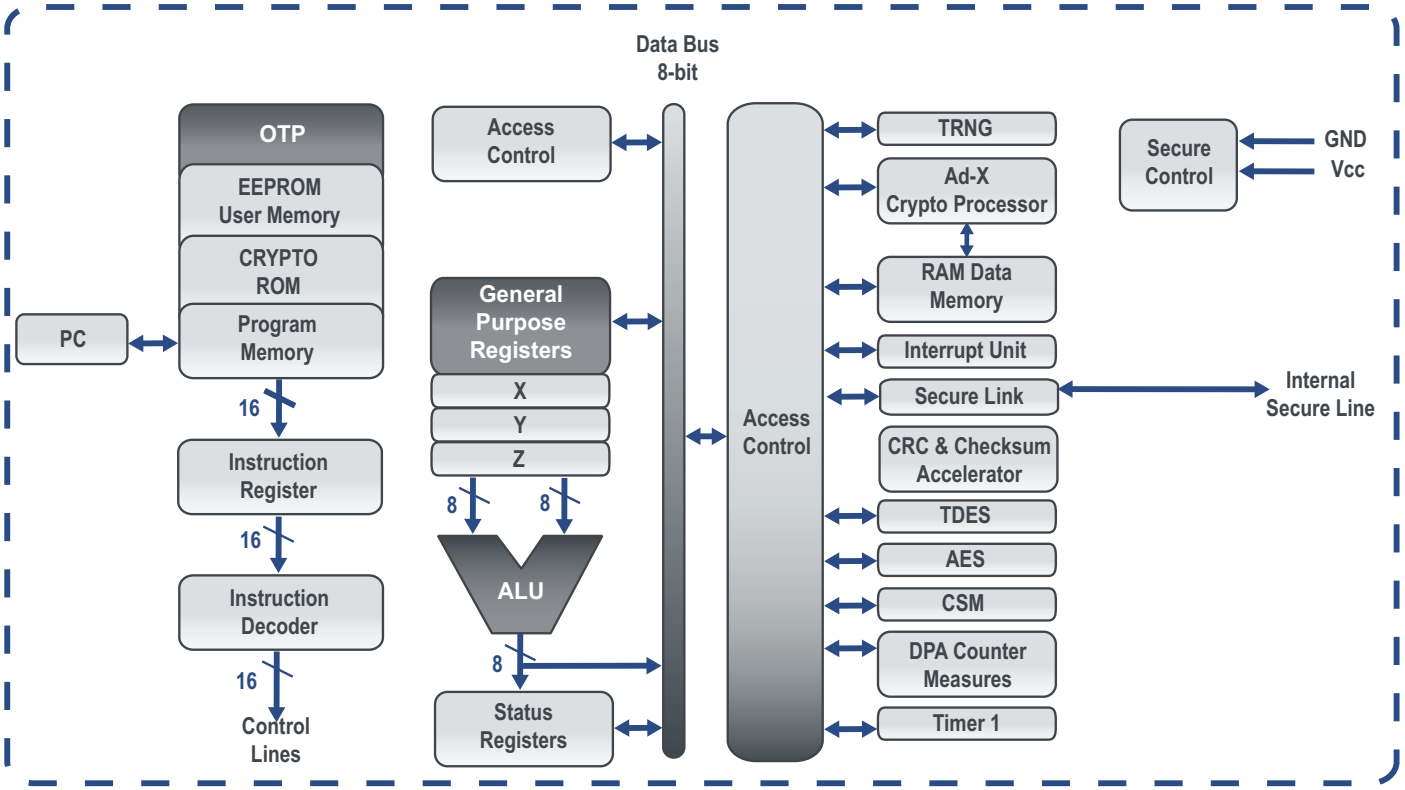
Figure 1 Master Core Architecture



Secure 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 2 Secure Core Architecture



6578ES – 28Sep16