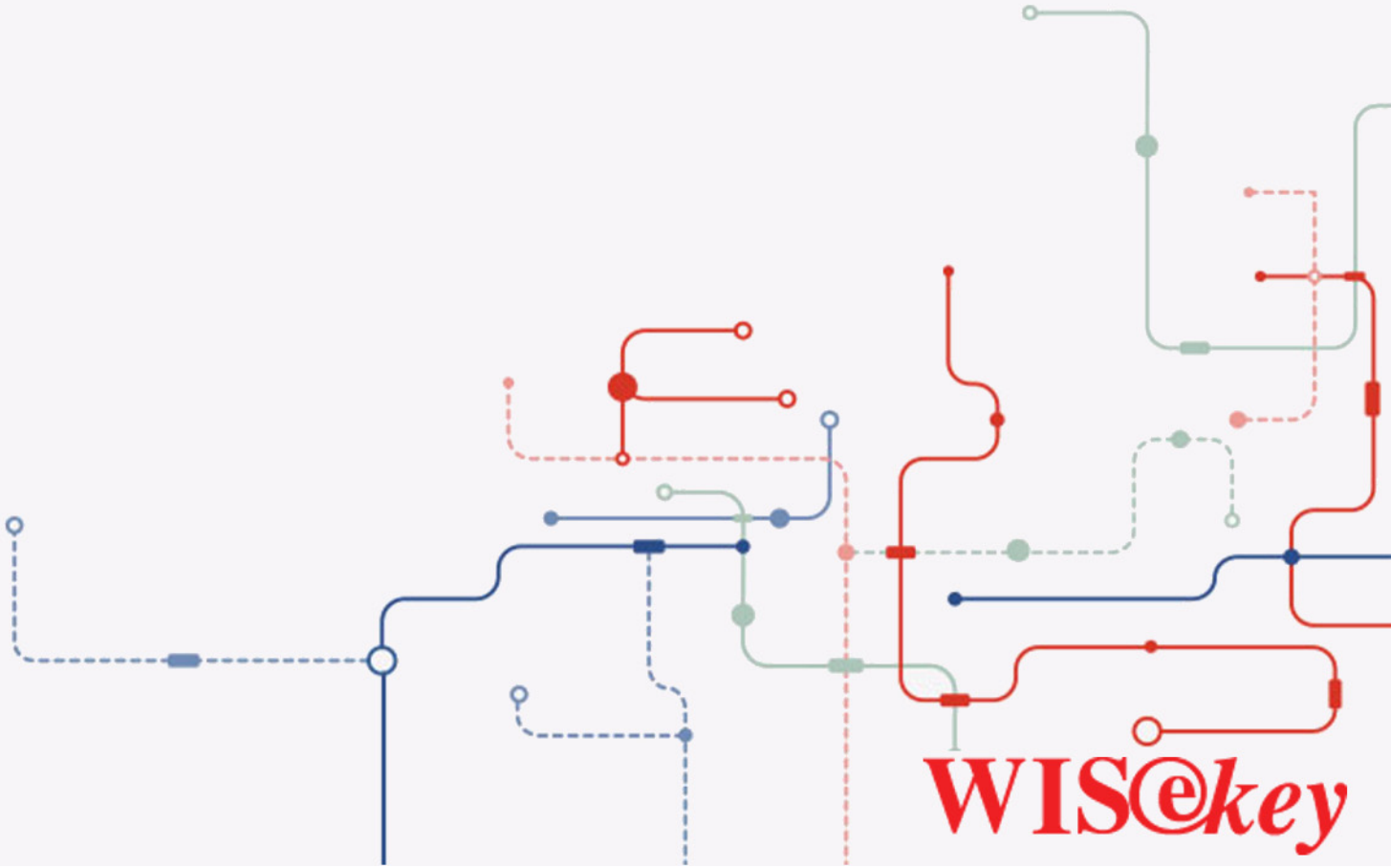
AT90SC20818RCFV

Summary Datasheet



Features

General

- High-performance, Low-power 8/16-bit Enhanced RISC Architecture
  - 135 Powerful Instructions (Most Executed in a Single Clock Cycle)
- Low-power Idle and Power-Down Modes
- Bond Pad Locations Conforming to ISO 7816-2
- ESD Protection to ± 5kV on ISO and ± 2kV on RF pins
- Operating Ranges: from 2.7V to 5.5V
- Compliant with EMV 4.3 Specifications and CQM
- Compliant with ICAO e-Passport Specifications
- Available in Wafers, Modules, Contactless Modules, Inlays and Industry-standard Packages
- Compatible with Printed Antennas (losses from 10 to 20 Ohms)
- Compatible with Half Antennas (Class 2)

Memory

- 208K Bytes of ROM Program Memory Including 32K Bytes with Specific Access
- 18K Bytes of EEPROM, Including 128 OTP Bytes and 384 Bit-addressable Bytes
  - 1 to 64-byte Program/Erase
  - 1 ms Program, 1 ms Erase
  - Endurance: 500,000 Write/Erase Cycles at 25°C
  - 10 Years Data Retention
  - EEPROM Erase Only Mode
  - Write EEPROM without or with Auto-Erase
- 6K Bytes of RAM + 256 Bytes of DMA dedicated RAM

Contactless Mode

- Contactless Interface Controller (CIC) with Full Support for ISO/IEC 14443 Type B Protocol
- Compliant with ISO14443 and ISO10373-6 Specifications
- On-chip Tuning Capacitance: 92pF
- Baud Rates: 106, 212 and 424 Kbps

Peripherals

- One I/O Port
- One ISO 7816 controller
  - Up to 625 kbps at 5 MHz
  - Compliant with T = 0 and T = 1 Protocols
- Programmable Internal Oscillator (Up to 30 MHz for Ad-X™ 2 and internal CPU Clock)
- Three 16-bit Timers
- Random Number Generator (RNG)
- 2-level, 8-vector Interrupt Controller
- Hardware DES and Triple DES 2 Keys, DPA and DEMA Resistant
- Hardware AES
- Code Signature Module
- CRC 16 & 32 Engine (Compliant with ISO/IEC 3309)
- 32-Bit Cryptographic Accelerator for Public Key Operations (Ad-X2 for Public Key Operations)
  - RSA, DSA, ECC, Diffie-Hellman

Security

- Dedicated Hardware for Protection Against SPA / DPA / DEMA / SEMA Attacks
- Advanced Protection Against Physical Attack, Including Active Shield, EPO, CStackChecker, Slope Detector, and Parity Errors
- Environmental Protection Systems
  - Voltage, Frequency and Temperature Monitors
  - Light Protection
- Secure Memory Management/Access Protection (Supervisor Mode)
- Start on Internal Oscillator
- No External Clock for Contactless Mode

Targeted Certifications

- Common Criteria EAL5+
- EMVCo
- FIPS 140-2

Development Tools

- Voyager Emulation Platform (ATV4Plus) to Support Software Development
- IAR Embedded Workbench® V4.30 Debugger or Above
- Software Libraries and Application Notes.

6598FS – 26Sep16

Description

The AT90SC20818RCFV is a low-power, high-performance, 8/16-bit microcontroller with ROM program memory, EEPROM data memory and a crypto-accelerator, based on an enhanced RISC architecture.

By executing powerful instructions in a single clock cycle, the AT90SC20818RCFV 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.

The AT90SC20818RCFV allows the linear addressing of up to 8M bytes of code and up to 16M bytes of data as well as a number of new functional and security features.

In addition to the 208K bytes of embedded ROM, the AT90SC20818RCFV features 18K bytes of high-performance EEPROM (fast erase/write time, high endurance).

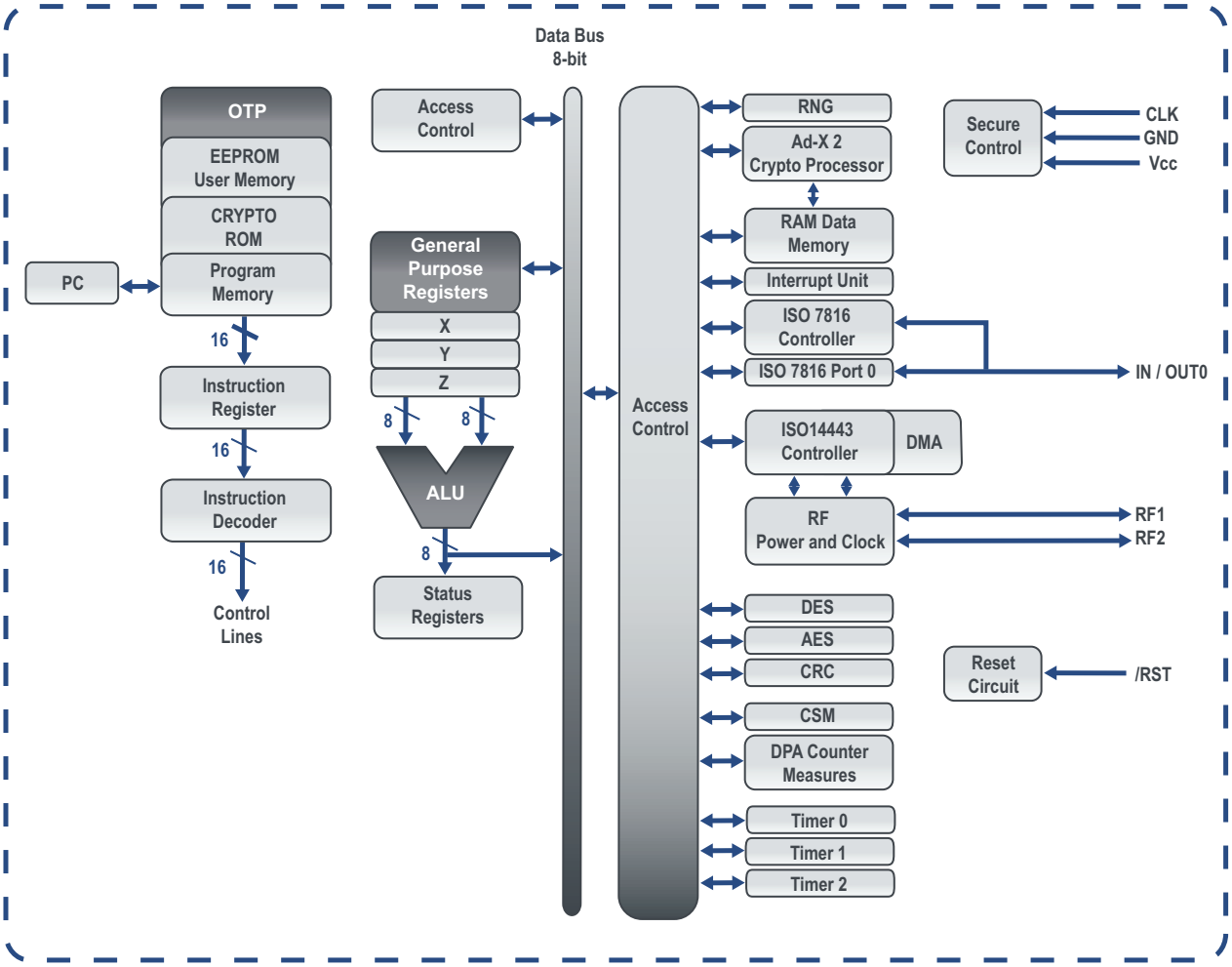
The ability to map the EEPROM in the code space allows parts of the program memory to be reprogrammed in-system. This technology combined with the versatile 8/16-bit CPU on a monolithic chip provides a highly flexible and cost effective solution to many smart card applications.

The cryptographic accelerator featured in the AT90SC20818RCFV is the new Ad-X2, a N-bit multiplier-accumulator dedicated to performing fast encryption and authentication functions. All cryptographic routines are executed on the CPU core which uses the Ad-X2 accelerator during encryption/decryption. Ad-X2 is based on a 32-bit technology, thus enabling fast computation and low power operation. Ad-X2 supports standard finite fields arithmetic functions (including RSA, DSA, DH and ECC) and GF(2N) arithmetic functions (including ECC).

Additional security features include power, frequency and temperature protection logic, logical scrambling on program data and addresses, power analysis countermeasures, and memory accesses controlled by a supervisor mode.

- A block diagram of the AT90SC20818RCFV is shown in Figure 1

Figure 1 AT90SC20818RCFV RISC CPU Core Architecture



6598FS – 26Sep16