ST22T064-A

Smartcard 32-Bit RISC MCU with 64 Kbytes EEPROM & USB 2.0 Full Speed Device Controller

DATA BRIEF

PRODUCT FEATURES

- 32-BIT RISC CPU WITH 24-BIT LINEAR MEMORY ADDRESSING
- 228 KBYTES USER ROM
- 16 KBYTES USER RAM
- 64 KBYTES USER EEPROM

32-BIT RISC CPU

- DUAL INSTRUCTION SET, JAVACARD™ AND NATIVE
- 4-STAGE PIPELINE
- 16 GENERAL PURPOSE 32-BIT REGISTERS, AND SPECIAL REGISTERS
- 4 MASKABLE INTERRUPT LEVELS
- SUPERVISOR AND USER MODES

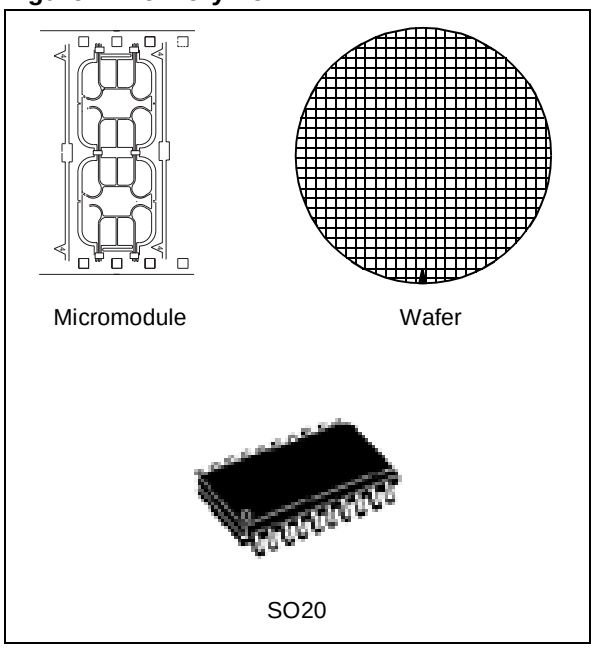
USB 2.0 FULL SPEED DEVICE CONTROLLER WITH ON CHIP CLOCK RECOVERY

- UP TO 12Mbits/s BANDWIDTH
- 16 DYNAMICALLY CONFIGURABLE ENDPOINTS
- ALL USB TRANSFER MODES SUPPORTED
- ISO / USB MODE DETECTION
- CCID AND ISO 7816-12 COMPLIANT

SECURITY

- CPU SECURITY INSTRUCTIONS
  - Dedicated instructions for DES and Triple DES implementation
  - Dedicated instructions (Multiply and Accumulate) for efficient implementation of modular arithmetic and elliptic curves based cryptosystems
  - CRC instruction (ISO 3309 16-bit Checksum)
- ENCRYPTION CO-PROCESSOR
- CPU DPA/SPA COUNTERMEASURES
- RANDOM NUMBER GENERATOR
- EEPROM FLASH PROGRAMMING MODE
- CLOCK AND POWER MANAGEMENT
- VOLTAGE AND CLOCK FREQUENCY SENSORS
- ADVANCED MEMORY PROTECTION
  - *Memory Protection Unit* for application firewalling and peripheral access control
  - Domain switching securely controlled by protected Context Stack
  - Native/Java, Code/Data memory attributes with 128-byte granularity
- FOUR WORKING STACKS
  - Java stack with both 16 and 32-bit accesses
  - User and Supervisor mode stacks
  - Security Context Stack

Figure 1. Delivery Form



For further information contact your local ST sales office.

CRYPTOGRAPHIC LIBRARY

The Crypto Library is provided as a separate ROM area with an access through a unique entry point. This library provides optimized -for the SmartJ core- and secured implementation of the following features:

- ASYMMETRICAL ALGORITHMS
  - RSA signature/verification
  - Prime number generation (up to 1024-bit)
  - RSA key computation (up to 2048-bit)
- HASH FUNCTION
  - SHA-1
- SYMMETRICAL ALGORITHMS
  - DES, Triple DES, AES

CRYPTOGRAPHY PERFORMANCE

The following table provides the cryptographic performances of the ST22T064-A based on ST Crypto Library.

Table 1. Preliminary Cryptographic Performances

Algorithm	Function	Time(1)
RSA 1024 bits	Signature with CRT	79.0 ms
	Signature without CRT(2)	242.0 ms
	Verification (e=0x10001)	3.6 ms
RSA 2048 bits	Signature with CRT	485.0 ms
	Signature without CRT	1.7 s
	Verification (e=0x10001)	11.0 ms
DES	Triple	18 µs
	Single	8 µs
TDES(3)	Triple (with keys loaded)	1.8 us
SHA-1	512-bit Block	194 µs
AES-128	Encryption including subkey computation	85 µs

1. Internal clock at 33 MHz
2. CRT: Chinese Reminder Theorem
3. TDES with encryption coprocessor

MEMORY

- HIGHLY RELIABLE CMOS EEPROM TECHNOLOGY
  - Error Correction Code for single bit fail within a 32-bit word
  - 10 years data retention, 500,000 Erase/ Write cycles endurance
  - 1 to 128 bytes Erase or Program in 2 ms typical
- HIGH PERFORMANCE MEMORY
  - Dual memory buses for data and instruction
  - Byte, Short (2) and Word (4) load and store
  - Address auto-increment

OTHER FEATURES

- HARDWARE ASYNCHRONOUS SERIAL INTERFACE (ASI)
  - 1M baud rate capability
  - 2 serial I/O ports compatible ISO 7816-3 T=0 and T=1
- 2 USER CONFIGURABLE 12-BIT AND 16-BIT TIMERS WITH INTERRUPT
- CENTRAL INTERRUPT CONTROLLER WITH UP TO 16 INPUT LINES
- EXTERNAL CLOCK FROM 1 MHz TO 10 MHz (ISO 7816-3 MODE)
- 1.62 V TO 5.5 V SUPPLY VOLTAGE (ISO 7816-3 MODE)
- 4V TO 5.5V IN THE USB MODE
- TEMPERATURE RANGE -25° C to +85° C
- POWER SAVING STANDBY MODE, SUSPEND (USB)
- ESD PROTECTION GREATER THAN 5000 V
- UNIQUE IDENTIFICATION PER DIE
- TYPICAL INTERNAL FREQUENCY UP TO 33 MHz
- SOFTWARE CONTROLLED CLOCK MANAGEMENT

DESCRIPTION

The ST22T064-A is a member of the SmartJ™ platform using a 32-bit Reduced Instruction Set Computer (RISC) core to execute both Native RISC instructions and JavaCard™ 2.x Technology instruction (byte codes) directly (See Figure 2. "SmartJ™ Platform EEPROM Architecture", on page 3).

Direct JavaCard™ byte code execution provides high performance advantage over processors that emulate the JavaCard™ byte code instruction set.

The USB 2.0 full speed device controller allows communication up to 12Mbits/s. The interface features 16 configurable endpoints and supports control, bulk, interrupt and isochronous transfer modes. This makes the ST22T064-A suitable for PC and network access control as well as multimedia applications such as secure multimedia content broadcast. The clock recovery eliminates the need for crystals or other external circuitry, thus allowing cost effective USB token design.

Memory and Peripheral accesses are controlled by a *Memory Protection Unit* that allows to implement firewalls between applications.

Memories are accessed via two different buses, allowing simultaneous accesses to code and data.

Memory load and stores can be performed at byte, short (2-bytes), or word (4-bytes) granularity, with optional pointer auto increment.

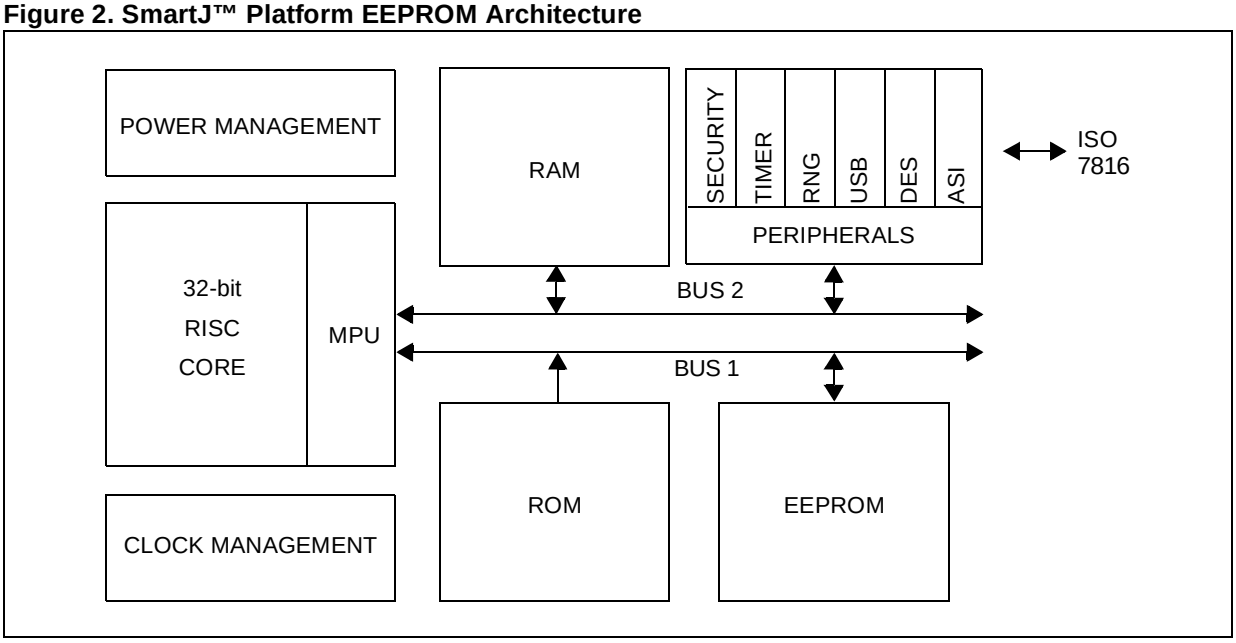
The ST22 core includes dedicated instructions to accelerate performances of the following algoriths:

– DES and Triple DES
– Modular Arithmetic on big numbers,
– Characteristic two field arithmetic to support efficiently Elliptic Curves,
– CRC 16-bit ISO 3309.

Cryptography performance can be increased for DES thanks to a dedicated DES / Triple DES accelerator.

The product has clock and power management, 2 User configurable Timers, a Central Interrupt Controller and a Random Number Generator.

Figure 2. SmartJ™ Platform EEPROM Architecture



The product has two execution modes. *Java* mode is used when JavaCard™ 2.x byte codes are being executed. *Native* mode is used for long JavaCard™ byte codes, Native methods and system routines. The processor enters Java mode when a dispatch (*DISP*) instruction is encountered. When executing in Native mode, there are two privilege levels, *User* and *Supervisor*. Some instructions can only be executed in *Supervisor* mode.

Instructions are of variable length, from 1 to 4 bytes in Native mode.

Special instructions exist for single-cycle stack operations, a frequent occurrence in Java code. Short branches and conditional branches within a 1 KByte block or the entire 16-MByte instruction space are supported. The product has four stages of pipeline in Native mode: fetch, decode, execute and write-back. In Java mode, there are five stages of pipeline: byte code-fetch, byte code-decode, decode, execute and write-back.

The CPU core has 16 32-bit general purpose registers, as well as special registers of variable length.

The chip also features a very high performance Asynchronous Serial Interface (ASI) to support high speed serial communication protocols compatible with ISO 7816-3 standard.

It is manufactured using the highly reliable ST CMOS EEPROM technology.

EMBEDDED SOFTWARE

The Hardware Software Interface (HSI) implements the Hardware abstraction layer. It consists of C interfaces to the EEPROM memory and peripherals. The drivers are:

– Non Volatile Memory
– Asynchronous Serial Interface
– USB
– Central Interrupt Controller
– Timer
– Random Number Generator
– Clock Manager
– Memory Protection Unit
– Sensors
– Encryption Coprocessor (DES)
– Security

Note:

– The HSI driver software layer is a C-oriented API allowing efficient and secure access to the peripherals and Non Volatile Memory for programming or erasing. It is the only way to access to the USB interface.
– Only the OS and JavaCard™ Virtual Machine (JVM) domains can access the HSI software layer (In the following the term OS will refer to the software layer that is directly interfaced to the HSI).

CRYPTOGRAPHIC LIBRARY

ST proposes a complete set of firmware subroutines to allow fast and easy implementation of cryptographic protocols. These subroutines have been optimized according to the ST22 core specificities and dedicated instructions. Security issues have been addressed to provide state of the art security. The whole library is located in a specific ROM area access through a single entry point. Following features are available through library:

■ ASYMMETRICAL ALGORITHMS:
  – Basic modular arithmetic for various lengths including modular product for odd modulus.
  – More elaborate functions (with separate fast and secure versions) such as exponentiation, RSA signatures and verifications for modulo length up to 2048 bits long.
  – Full internal RSA key generation. This guarantees that the secret key will never be known outside the chip and will contribute to the overall system security,
  – Random number generation of big size,
  – SHA-1.
■ SYMMETRICAL ALGORITHMS
  – DES, Triple DES including key schedule,
  – AES with standalone key schedule for lenght 128, 192 and 256.

SOFTWARE DEVELOPMENT ENVIRONMENT

Modularity, flexibility and methodology are the key words for the SmartJ™ Development Tools Platform. Using the same interface, the developers are able to create, compile and debug a project.

The SmartJ™ Integrated Development environment (IDE) includes:

– A code Generation chain: C/C++ compiler, assembler and linker. The assembler supports both native and JavaCard™ instruction sets.

– An instruction set simulator, a cycle accurate simulator, a C/C++ source level debugger. Software and Hardware tools allow to efficiently generate, then validate all code and application embbeded softwares for the SmartJ™ platform.

Figure 3. SmartJ™ IDE

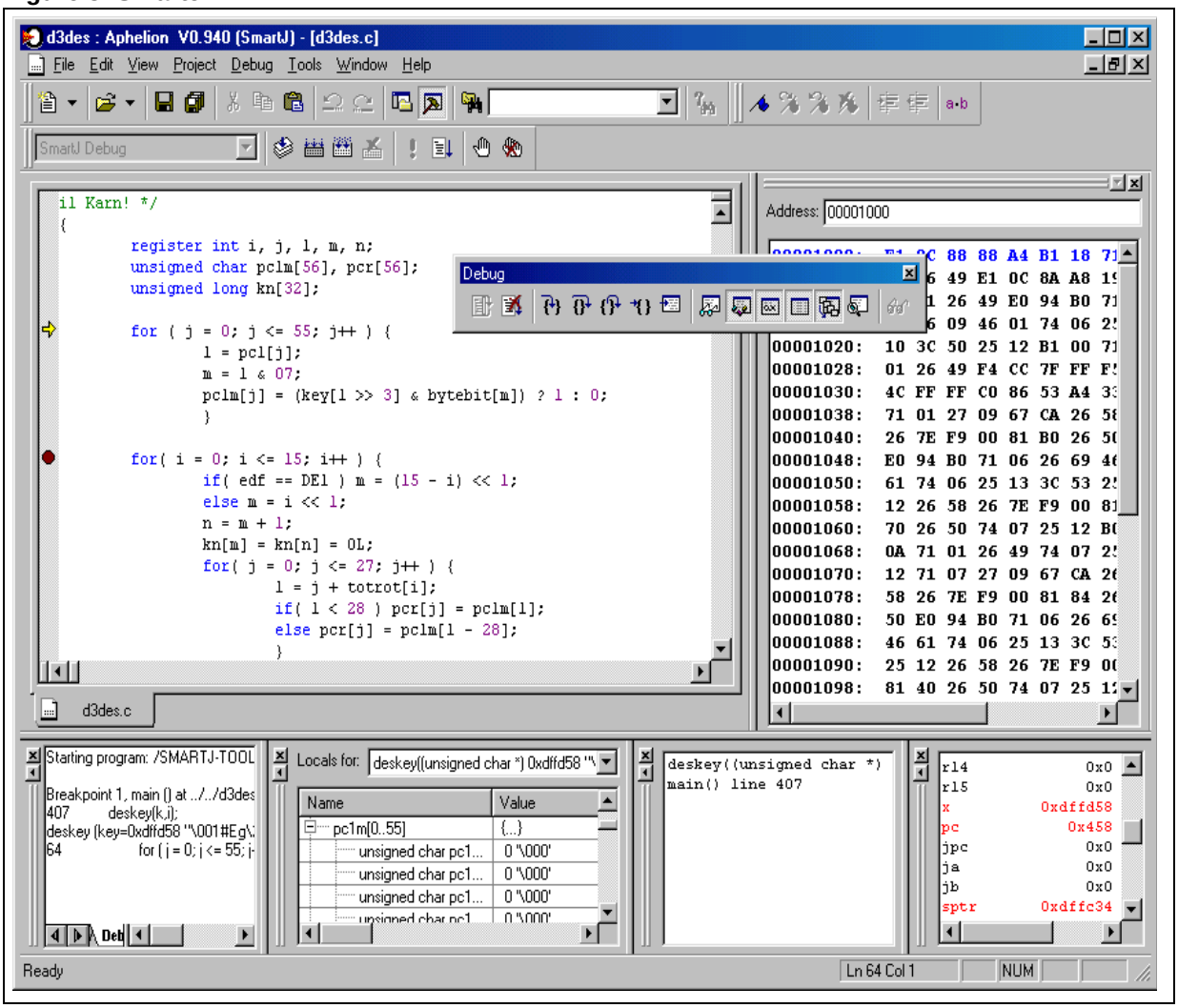


Figure 4. SmartJ™ Code Generation Tools

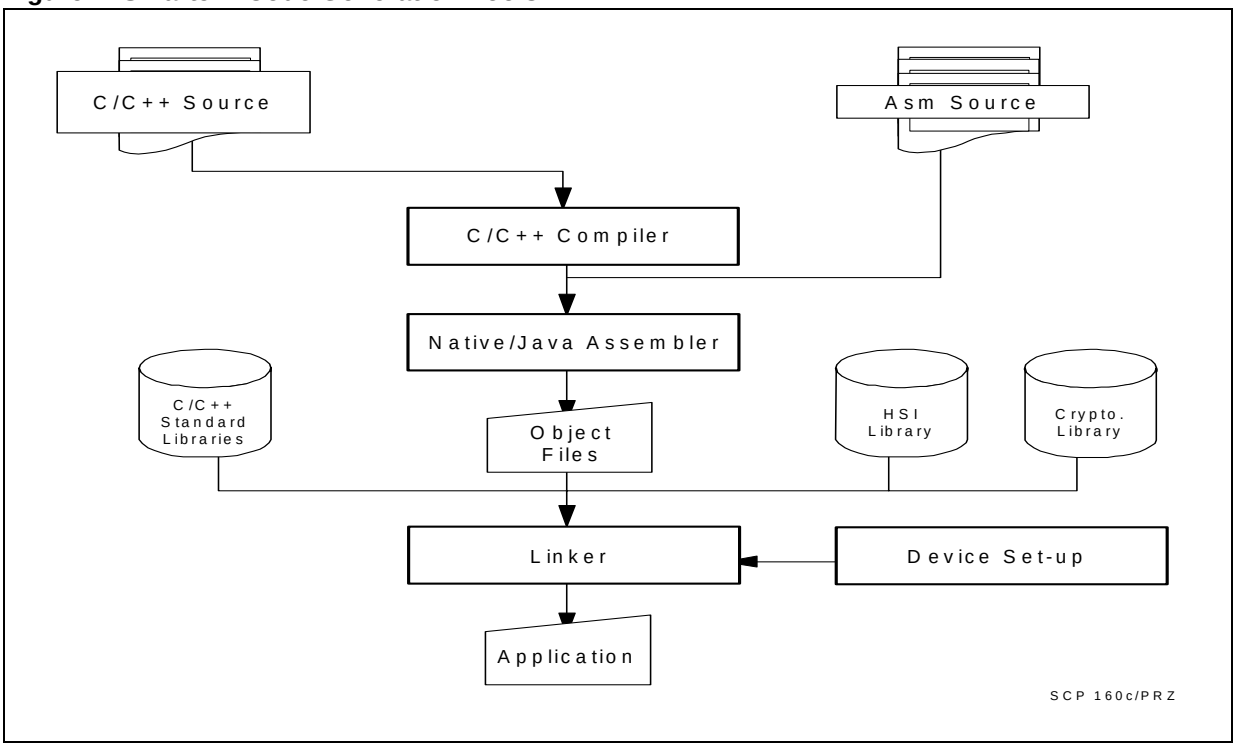


Figure 5. SmartJ™ Code Validation Tools