360KB High Performances Flash Smart Card IC – SPI-MS / GPIO

Environment
- Voltage Supply Class A, B, C: 1.8V, 3V, 5.0V ± 10%
- SIM-SPI: Class A, B and C compatible
- -25 to +85 ^{0}C Operating Temperature
- Max supply current 10mA @ 20MHz, Class A
- Max supply current 6mA @ 20MHz, Class B
- Max supply current 4mA @ 20MHz, Class C
- ISO7816-3 pads > 4 kV ESD Protection HBM
- SPI-GPIO pads > 2 kV ESD Protection HBM

CPU
- Software compatible Intel 80251 (MCS251)
- Accelerated 16 bit CPU Architecture
- Up to 20 MHz internal CPU clock

Idle Modes
- Idle and Stop mode selectable modes
- NVM update operation with CPU in idle mode
- IO Transmission and Reception with CPU in idle mode
- Max Idle current / Clock stopped: 100 uA

Security
- Hardware Random Number Generator
- Hardware DES/TDES module
- CRC16 module
- Unique chip identification number
- Notification of tampering
- IC operates under regulated voltage and internal clock
- Under / Over voltage sensors (Vcc)

Memory Control
- General Purpose Non Volatile Memory: GPNVM
- Memory Management Protection Mechanism
- Memory management HW logical to physical (LOG2PHY)
- Ultra Fast Byte program
- Fast GPNVM Page Erase time

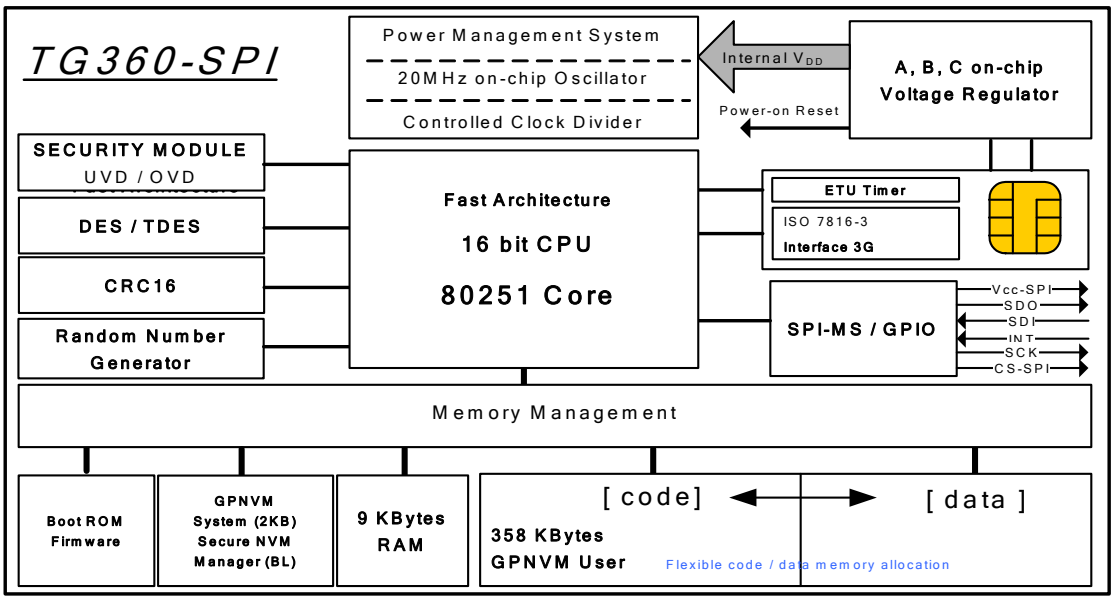
ISO 7816-3 interface
- ISO 7816-3 compliant electrical interface
- ISO 7816-3 compliant T=0 and T=1 protocols
- ETU Timer/Counter

SPI-MS / GPIO :
- SPI-Master mode 4 wires
- SPI-Slave mode 4 wires
- GPIO 6 IOs
- Vdd-SPI power supply output
- SPI-INT signal connect to MCS251 interrupt controller

Memories
- 9KB RAM
- 358 KB User GPNVM256 = 256B/page
- 2KB System GPNVM= 16 Pages of 256 B
- GPNVM data retention: 10 years
- GPNVM Endurance E/W > 100 Kcycles
- Secure boot loader T=0 compatible

Chip Forms
- 8” Wafer sawn or unsawn
- Back grinding and distressing options
- Modules

Typical Application:
- Smartcards with sensors interfaces
- USIM cards 128KB
- JavaCard based platform



Introduction

TG360-SPI is a member of the Theseus family of devices designed specifically for smart card applications and Java Card technology. It is software compatible with the industry standard MCS251 micro-controller. Computing performances are powering JavaCard based applications with large provision of memory resources seen thru linear Von Neumann space up to 24MB.

Security of the family of devices makes them particularly suitable in electronic commerce and sensitive data areas. This is accomplished in hardware, with not only protection against out of parameter operation of the device, but hardware memory management to protect against software security attacks. The CPU clock is derived from its own internal oscillator, so preventing attacks by clock manipulation, or extrapolating program execution by monitoring current variations on clock edges.

The need to support the emerging multifunction cards requires that the device under software control can download an application and run it when the device is in the field embedded in a plastic card. This application can be in the form of a script to be executed by an interpreter or as a raw binary directly executed by the processor. The device has to be protected against the downloading of attack software designed to corrupt or uncover the working or data contained in the device. Traditionally this has been a software function, which relies on the total integrity of the embedded software. The TG360-SPI implements the first level of protection in hardware.

A dynamic memory protection mechanism is relying on a flexible border between code and data space.

The General Purpose Non Volatile Memory concept allows reaching ultra low cost implementation of traditional 128KB EEPROM smart card ICs and more. All your efforts to save code footprint are optimizing your end product performances.

Serial interface

TG360-SPI offers a unique serial interface compliant with the ISO 7816-3 specification with several modes implemented allowing serial connections at 9600 up to 357K bits per second at 3.57MHz. TG360-SPI supports T=0 asynchronous half duplex character transmission protocol, T=1 asynchronous half duplex block transmission and a proprietary T=14 protocol used for fast loading of Code into the OTP by the card manufacturer. It handles minimum guard time requirements between characters specified by ISO7816-3 specification automatically. TG360-SPI is designed to be compatible with the ISO7816-3 specification defining the characteristics of Integrated Circuit Cards commonly referred to as smart cards.

Extended IOs provision SPI-MS and GPIO

SPI Master interface 4 wires is available to interface SIM device with external peripherals. INT input allows to interrupt MCS251 controller to handle special event if necessary.

Random Number Generator

The on chip random number generator is passing test based on Fips140-2 criteria, providing a rapid stream of truly random numbers. This allows use of the random numbers generated beyond just the provision of numbers for randomising transmissions or generating keys.

DES/TDES/3KDES and CRC16 Hardware modules

Hardware acceleration of DES / Triple DES and 3 Keys DES encryption decryption algorithms provide an efficient way to protect application data and code. It supports ECB and CBC modes. In addition, CRC16 hardware module allows the verification of data integrity.

Clocks

TG360-SPI has its own internal oscillator this allows the core of the device to be independent of the external clock. The processor can also be clocked much faster than the IO CLK signal. This ensures the elimination of fraudulent attacks involving frequency jitter and unequal mark space ratios. The internal clock generator is connected to the core via a divider that is under the control of the software. This allows the Operating System writer to control the trade off between execution speed and power drawn by the device. Extending battery life in hand help applications where slow interfaces are involved.

Anti tampering

The TG360-SPI has extensive anti tampering provision including the monitoring of the connection to the device to ensure that deviations beyond a prescribed criteria result in the device being closed down before its operating conditions are violated.

On chip voltage regulators

Several on chip regulators isolate the various elements of the device from variations and fluctuations in the supply voltage. This allows elements to be characterised precisely, as they operate at one fixed voltage, which in turn maximises the endurance of the device.

Technology

This product is using superior Flash memory SuperFlash Technology licensed from SST and SuperFlash is a registered trademark of SST (Silicon Storage Technology Inc.).

Technical Data

Absolute Maximum Ratings

Parameter	Symbol	Limit Values			Unit
		min	typical	max	
Supply Operating Volt	V_{cc}	-0.3		6	V
Voltage at remaining pin	V_{pin}	V_{ss} –0.3		V_{cc}+0.3	V
Power dissipation	P_{tot}			+60	mW
Storage temperature	I_{ccI}	-40		+125	°C

DC Characteristics

Parameter	Symbol	Limit Values			Unit
		min	typical	max	
Operating temperature	T_A	-25		+85	°C
Supply Voltage Class A,B	V_{cc}	1.62		5.5	V
Supply Current Class B	I_{cc}			6 (Note 1)	mA
Supply Current Class C (SPI Idle)	I_{cc}			4 (Note 1)	mA
Supply Current idle	I_{ccI}			200 (Note 2)	µA
Supply Current stopped	I_{ccS}			100 (Note 3)	µA

Note 1: The supply current refers to external clock frequency of 5 Mhz
Note 2: The supply current at 3.3V and a clock frequency of 1 Mhz, at +25 ^{0}C
Note 3: The supply current at 3.3V and +25 ^{o}C

IO pin:

Parameter	Symbol	Conditions	min	max	Unit
H input voltage	V_{IH}	I_{Ihmax} =±20µA	0.7 * V_{cc}	V_{cc}	V
L input voltage	V_{IL}	$I_{IL\ max}$ =±20µA	-0.3	0.8	V
H output voltage (Note 1)	V_{OH}	I_{Ohmax} = +20µA	0.7 * V_{cc}	V_{cc}	V
L output voltage	V_{OL}	I_{Olmax} = -1mA	0	0.4	V
Rise Fall Time	t_r, t_F	C_{IN} = C_{OUT} = 30 pF		1	µS

NOTE 1: Assumes 20KΩ Pull up resistor on interface device

Clock (CLK)

Parameter	Symbol	Condition	Min	Max	Unit
H output voltage	V_{OH}	I_{Ohmax} = +20 µA	V_{cc}-0.7	V_{cc}	V
L output voltage	V_{OL}	I_{Olmax} = -20µA	0	0.5	V
Rise Fall Time	t_r, t_F	C_{IN} = C_{OUT} = 30 pF		9% CLK period	

Reset(RST)

Parameter	Symbol	Condition	Min	Max	Unit
H output voltage	V_{OH}	I_{Ohmax} = +20 µA	V_{cc}-0.7	V_{cc}	V
L output voltage	V_{OL}	I_{Olmax} = -20µA	0	0.6	V
Rise Fall Time	t_r, t_F	C_{IN} = C_{OUT} = 30 pF		400	µs