256KB Flash Smart Card IC + Crypto

Environment
- Voltage Class A, B and C : 1.8V, 3-5V supply ± 10%
- -25°C to +85°C operating temperature
- Max supply current 10 mA at 5.5 V and 30 MHz
- Max supply current 6 mA at 3.3 V and 30 MHz
- Max supply current 4 mA at 1.8 V and 10 MHz
- > 4 KV ESD Protection HBM

CPU
- Software compatible CMOS 80X51 industry standard
- "far" addressing support extending 'xdata' up to 8MB
- Accelerated architecture with 16 bit CPU performance level
- Linear code / data addressing (no bank switching)
- Up to 30 MHz internal CPU clock

Idle Modes
- Idle and Stop mode selectable modes
- NVM operation possible with CPU in idle mode
- IO Transmission and Reception with CPU in idle mode
- Max idle current 200 µA

Cryptography Resources
- DES / TDES Hardware accelerator
- CBC mode Hardware acceleration
- Hardware Random Number Generator FIPS140-2

Memory Control
- Memory Management Unit (MMU) + HW Firewall
- Memory physical access rights management
- Extended addressing capability with Java Mode
- EEPROM Erase write control
- EEPROM Fast program in FLASH Mode 40 µs / Byte
- EEPROM Multiple Page Erase up to 128 Bytes
- EEPROM Fast write in Flash mode
- OTPROM Bank Erase (32KB)
- FLASH Block Erase (2KB)

I/O
- ISO 7816-3 compliant electrical interface
- ISO 7816-3 compliant reset and response T=0 T=1 protocols

Security
- OTPROM / Flash block physical access rights
- CRC16 module hardware accelerator ISO3309
- Unique chip identification number
- Notification of tampering
- Out of frequency, voltage, temperature detection
- Internal clock and voltage generation
- DPA/SPA resistance mechanisms
- Security target EAL4+

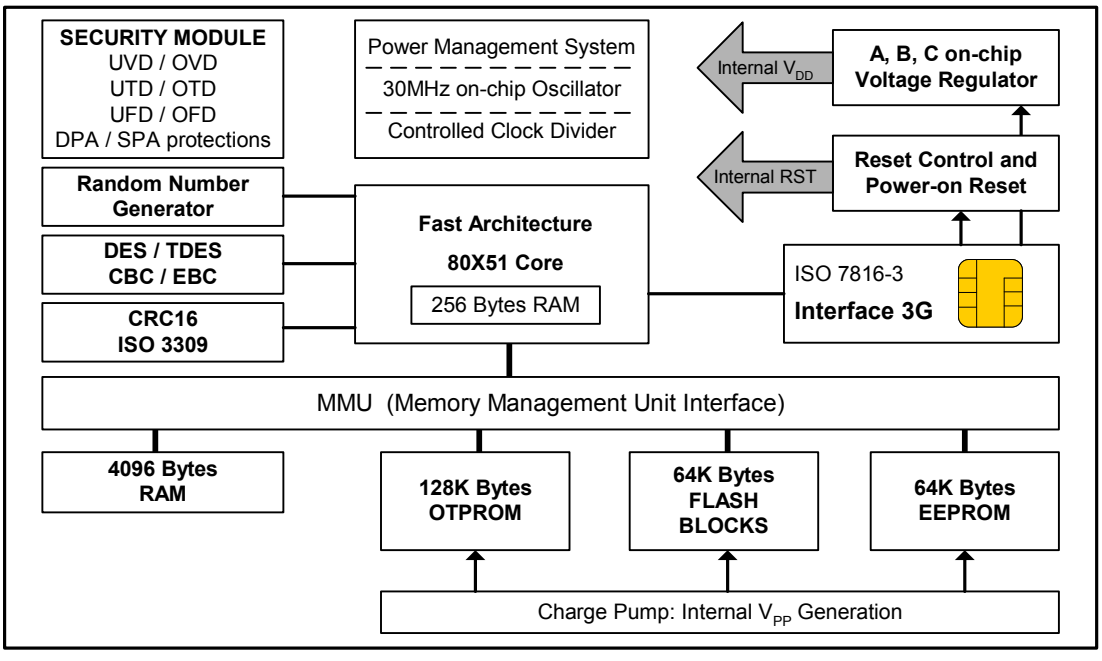
Memory
- 4KB XRAM +256B Internal RAM
- 128KB OTPROM 4 blocks of 32KB
- 64KB FLASH BLOCK 32 blocks of 2KB
- 64KB EEPROM
  - 10 year data retention
  - >300k read write cycles

Delivery form
- Backlapped and distressed 8" wafers to 180 µm
- Options: Sawn wafers on frame, Modules

Development kit
- Emulation platform (EME4652) fully integrated in Keil uVision2 Debugger with all debugging facilities
- Starter Kit EMSK4600 with uVision2 integration:
  - OTP, Flash blocks, EEPROM code download
  - EEPROM data download (personalization)

Applications
- Mobile communication : GSM: Phase 2, 2+ WIB, OTA, WLAN GPRS, UMTS, CDMA, Java Card Platform
- Banking, Health, loyalty, membership cards

Block Diagram



Introduction
EMTCG256-3G is a member of the Theseus family of devices designed specifically for smart card applications. It is software compatible with the industry standard 8051 micro-controller, to guarantee the maximum availability of qualified software. The hardware implementation of the core is a modern design not relying on microcode, with an increase of up to 4 times on a standard 8051's clocks per instruction.

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 EMTCG256-3G implements the first level of protection in hardware. This maximizes the security of the device, and allows the reusability of developed certified code, by isolating it from the actual hardware implementation of the device. This protection mechanism allows for a Secure Operating System to be embedded into the device at manufacture, which has access rights to features of the device that are denied to applications that can be loaded into the device at manufacture or in the field.

The Secure Operating System allocates to each application programme, areas of the memory resources of the device. The hardware then ensures that when the application code is executing only accesses to these designated spaces are made.

An extension of application mode has been developed to facilitate Java Card virtual machine integration.

With up to a 99KB (RAM+FLASH+ROM) of on chip memories EMTCG256-3G eradicates the need for memory bank switching either for data and code space. This is maximizing computing performances as well as code density of you application allowing Smart Card to integrate more features.

In systems where application isolation is not needed, the security mechanism acts as a general protection unit trapping software errors.

Non Volatiles Memories
The use of flash blocks of with 2kB increments configurable for code or data, allows to address different larger market range with a single product.

Serial interface
EMTCG256-3G 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. EMTCG256-3G 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. EMTCG256-3G is designed to be compatible with the ISO7816-3 specification defining the characteristics of Integrated Circuit Cards commonly referred to as smart cards.

DES/TDES
High performance symmetric encryption / decryption algorithm can be achieved using DES and Triple DES on chip HW Accelerator, this engine could be used as well in EBC and CBC modes. The intrinsic security of this DES implementation can be reinforced using SPA/DPA protection mechanisms to achieve very high level of security.

Random Number Generator
The on chip random number generator is fully Fips140-2 compliant, providing a rapid stream of truly random numbers. This allows use of the random numbers generated beyond just the provision of numbers for randomizing transmissions or generating keys.

Clocks
EMTCG256-3G 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 EMTCG256-3G 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 characterized precisely, as they operate at one fixed voltage, which in turn maximizes 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	
Ambient temperature	T_A	-25		+85	°C
Supply Voltage Class A,B	V_{cc}	2.7	3 / 5	5.5	V
Supply Voltage Class C	V_{cc}	1.62	1.8	1.98	V
Supply Current Class B	I_{cc}			6 (Note 1)	mA
Supply Current Class C	I_{cc}			4 (Note 1)	mA
Supply Current idle	I_{ccI}			200 (Note 2)	µA

Note 1: The supply current refers to clock frequency of 5 Mhz
Note 2: The supply current at 3.3V and a clock frequency of 1 Mhz, at +25°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 3)	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} = 30pF		1	µS

Note 3: Assumes 20KΩ Pull up resistor on interface device

Clock (CLK)

Parameter	Symbol	Condition	Min	Max	Unit
H output voltage	V_{OH}	I_{Ohmax} = +20µA	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} = 30pF		9% CLK period	

Reset(RST)

Parameter	Symbol	Condition	Min	Max	Unit
H output voltage	V_{OH}	I_{Ohmax} = +20µA	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} = 30pF		400	µs