



## 128KB Flash Smart Card IC + Cryptography Engine

### Environment

- ☐ Voltage Supply Class A, B: 3.0V to 5.0V  $\pm$  10%
- ☐ -25 to +85 °C Operating Temperature
- ☐ Max supply current 6mA @ 30MHz, Class B
- ☐ > 4 kV ESD Protection HBM

### CPU

- ☐ Software compatible CMOS 80X51 industry standard
- ☐ Local RAM 256 B (data, idata memory spaces)
- ☐ "far" addressing support extending 'xdata' up to 8MB
- ☐ Accelerated architecture with 16 bit CPU performance level
- ☐ 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 uA

### Cryptography Resources

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

### Security

- ☐ Unique chip identification number
- ☐ Notification of tampering
- ☐ Internal clock generation
- ☐ IC operates under regulated voltage
- ☐ DPA/SPA resistance mechanisms
- ☐ Under / Over voltage sensors (Vcc)
- ☐ CRC Hardware module featuring CRC16 and ISO3309 CRC

### Memory Control

- ☐ Memory Management Unit (MMU)
- ☐ Code / Data flexible memory partitioning thanks to GPNVM512 General Purpose NV Memory
- ☐ Application Secure OS partitioning (HW Firewall)
- ☐ Extended addressing capability with Java Mode for optimal memory mapping
- ☐ EEPROM and GPNVM512 Fast Byte program: 40 us / Byte
- ☐ EEPROM Erase write control
- ☐ EEPROM Write in FLASH Mode
- ☐ EEPROM Multiple Page Erase up to 128 Bytes

### I/O

- ☐ ISO 7816-3 compliant electrical interface
- ☐ ISO 7816-3 compliant reset and response T=0 T=1 protocols

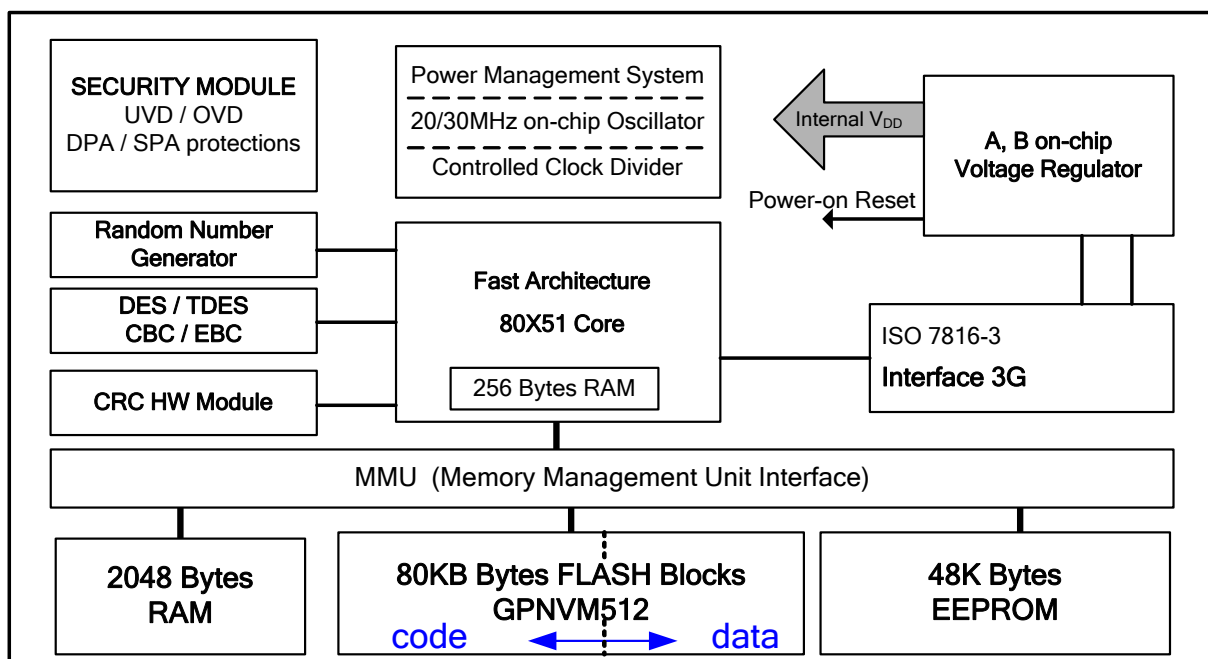
### Memories

- ☐ 2048 bytes RAM (xdata space)
- ☐ 80KB GPNVM512 (General Purpose Non Volatile Memory with 512B / Page)
- ☐ 48KB EEPROM
- ☐ 10 year data retention for EEPROM / GPNVM512
- ☐ EEPROM, GPNVM512 Endurance: 100 K cycles

### Chip Forms

- ☐ 8" Wafer sawn or unsawn
- ☐ Back grinding and distressing options
- ☐ 180 microns max thickness
- ☐ Modules

- ✓ EMTCG128-3G is Software Compatibility with EMTG256-3G
- ✓ Emulation and Debug Development tools fully integrated within Keil uVision2





## Introduction

EMTCG128-3G 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 EMTCG128-3G implements the first level of protection in hardware. This maximises 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.

With up to a 130KB (RAM+GPNVM512+EEPROM) of on chip memories EMTCG128-3G provides highly flexible memory partitioning between code and data. So called GPNVM512 standing for General Purpose Memory could be efficiently used to host data or code. Its 512 bytes page size offers very compact memory usable as well for code and data storage.

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.

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

## Serial interface

EMTCG128-3G 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. EMTCG128-3G 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. EMTCG128-3G 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 randomising transmissions or generating keys.

## Clocks

EMTCG128-3G 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 EMTCG128-3G 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 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. 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      | $I_{ccl}$ | -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 | $V_{cc}$  | 2.7          | 3 / 5   | 5.5          | V    |
| Supply Current Class B   | $I_{cc}$  |              |         | 6 (Note 1)   | mA   |
| Supply Current idle      | $I_{ccl}$ |              |         | 200 (Note 2) | μA   |
| Supply Current stopped   | $I_{ccs}$ |              |         | 100 (Note 3) | 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

Note 3: The supply current at 3.3V and +25 °C

**IO pin:**

| Parameter                 | Symbol     | Conditions                 | min            | max      | Unit |
|---------------------------|------------|----------------------------|----------------|----------|------|
| H input voltage           | $V_{IH}$   | $I_{Ihmax} = \pm 20 \mu A$ | $0.7 * V_{cc}$ | $V_{cc}$ | V    |
| L input voltage           | $V_{IL}$   | $I_{ILmax} = \pm 20 \mu A$ | -0.3           | 0.8      | V    |
| H output voltage (Note 1) | $V_{OH}$   | $I_{Ohmax} = +20 \mu A$    | $0.7 * V_{cc}$ | $V_{cc}$ | 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 | $V_{OH}$   | $I_{Ohmax} = +20 \mu A$    | $V_{cc} - 0.7$ | $V_{cc}$      | V    |
| L output voltage | $V_{OL}$   | $I_{Olmax} = -20 \mu A$    | 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 | $V_{OH}$   | $I_{Ohmax} = +20 \mu A$    | $V_{cc} - 0.7$ | $V_{cc}$ | V    |
| L output voltage | $V_{OL}$   | $I_{Olmax} = -20 \mu A$    | 0              | 0.6      | V    |
| Rise Fall Time   | $t_r, t_f$ | $C_{IN} = C_{OUT} = 30 pF$ |                | 400      | μS   |

EM Microelectronic-Marín SA (EM) makes no warranty for the use of its products, other than those expressly contained in the Company's standard warranty which is detailed in EM's General Terms of Sale located on the Company's web site. EM assumes no responsibility for any errors which may appear in this document, reserves the right to change devices or specifications detailed herein at any time without notice, and does not make any commitment to update the information contained herein. No licenses to patents or other intellectual property of EM are granted in connection with the sale of EM products, expressly or by implications. EM's products are not authorized for use as components in life support devices or systems.