96kB FLASH Memory Smart Card IC

Environment
- ❑ Single 3.0V to 5.0V supply ± 10%
- ❑ -25 to +85 ^{0}C operating temperature
- ❑ Max supply current 10mA
- ❑ > 4 kV ESD Protection HBM

CPU
- ❑ Software compatible CMOS 8051 industry standard
- ❑ High speed non standard architecture with 16 bit CPU performance level
- ❑ Up to 20 MHz internal CPU clock
- ❑ Idle and stop mode selectable modes

Memory Control
- ❑ Memory Management Unit (MMU)
- ❑ Application Secure OS partitioning
- ❑ EEPROM Erase write control
- ❑ EEPROM with Flash mode

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

Security
- ❑ Out of frequency, voltage detection
- ❑ Unique chip identification number
- ❑ Notification of tampering
- ❑ Hardware Random Number Generator
- ❑ Internal clock generation
- ❑ DPA/SPA resistance mechanisms

Memories
- ❑ 2048 bytes Ram
- ❑ 64KB OTPROM
- ❑ 32KB EEPROM
  - ⇨ 10 year data retention
  - ⇨ Endurance >100k write cycles
- ❑ 1.5 KB ROM (Bootrom)

Chip forms
- ❑ Wafer sawn or unsawn
- ❑ Back grinding and distressing options
- ❑ 180 microns max thickness
- ❑ Die size < 20 mm^2
- ❑ Modules

Applications
- ❑ Mobile communication : Phase 2, 2+, 2.5
- ❑ Banking
- ❑ Health, loyalty, membership cards

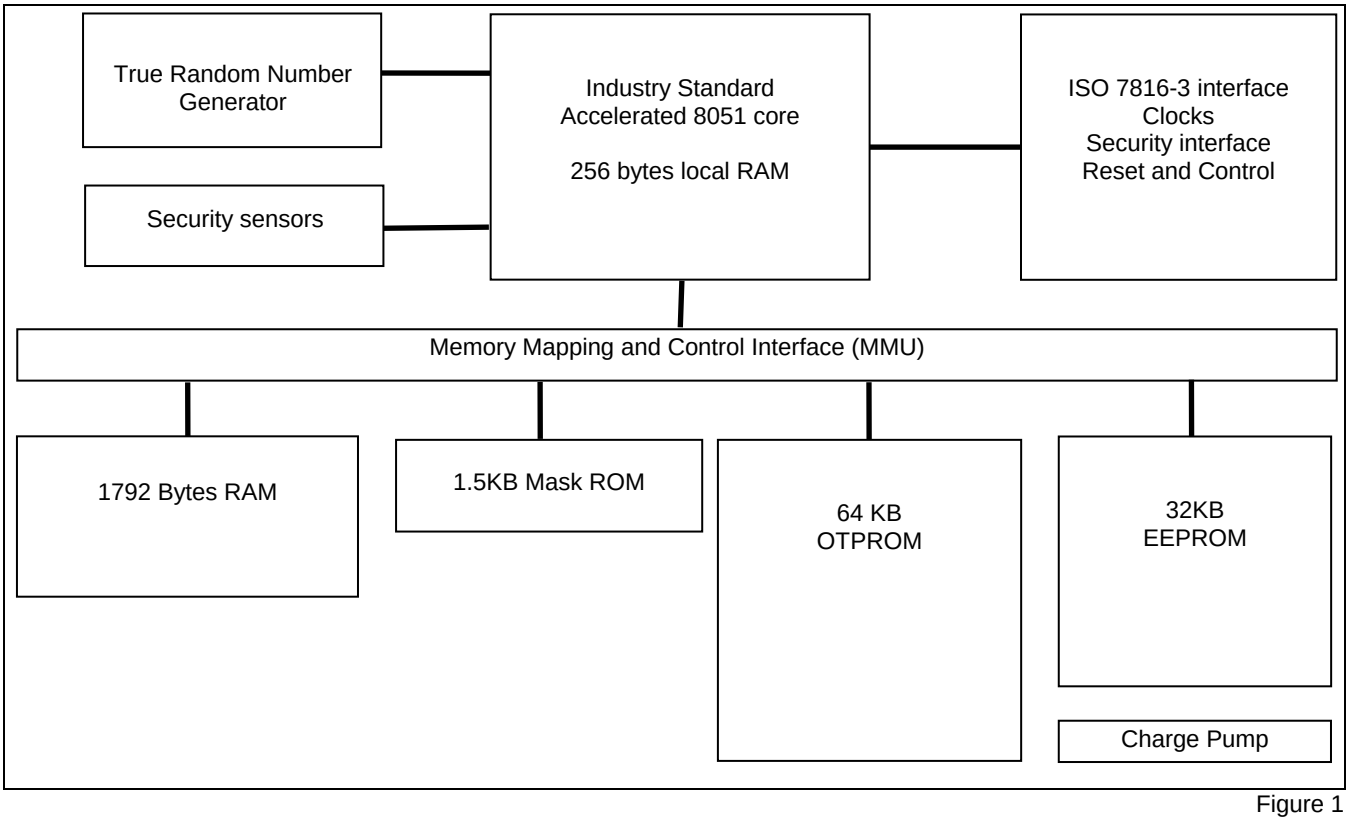

Figure 1

Introduction
The EMTG96-3G, also known as THESEUS™ Gold 96 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. EMTG96-3G 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.

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
EMTG96-3G 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. EMTG96-3G 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. The THESEUS™ family is designed to be compatible with the ISO7816-3 specification defining the characteristics of Integrated Circuit Cards commonly referred to as smart cards.

Random Number Generator
The on chip random number generator is fully Fips140-1 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
EMTG96-3G 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
EMTG96-3G 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.

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	V_{cc}	2.7	3 / 5	5.5	V
Supply Current	I_{cc}			6 (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 at 3.3V refers to a 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