# THESEUS® GOLD 48 PUBLIC DATASHEET

## Emosyn Worldwide Locations

### Headquarters, Administration, Legal, Finance, Operations

7 Commerce Drive
Danbury, CT
06810-4169
U.S.A.
tel. +1 203 794 1100
fax +1 203 830 4116

### Worldwide Sales & Marketing, Customer Service, Technical Support

Spinners Court
53-55 West End
Witney, Oxfordshire
OX28 1NH
U.K.
tel. +44 1993 700 327
fax +44 1993 700 299

### Engineering and Design

617 River Oaks Parkway
San Jose, CA 95134
U.S.A.
tel. +1 408 526 9400
fax +1 408 526 1651

### Asia Pacific Sales and Technical Support

25 International Business Park
04-75 German Centre
Singapore 609916
tel. +65 562 8200
fax +65 562 8201

Or visit our website at www.emosyn.com.

# 1 Table of Contents

# 2 Theseus Gold 48 Summary

The Theseus Gold 48 integrated circuit is a member of the Theseus Gold family of devices designed specifically for smart card applications. It is software compatible with the industry standard 8051 8-bit microprocessor, to guarantee the maximum availability of tested 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. As with all Theseus Gold smart card ICs, it is fully compatible with the ISO-7816 specifications.

Security of the family of devices makes them particularly suitable in electronic commerce and areas of sensitive data. This is accomplished in hardware, with protection against out of parameter operation of the device, and also hardware memory management to protect against software security attacks. The CPU clock is derived from its own internal oscillator, which prevents attacks by clock manipulation, or extrapolating program execution by monitoring current variations on clock edges.

The need to support multifunction cards requires that the device be able to download an application and run it under software control when the device is in the field embedded in a smart card. 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 Theseus Gold 48 implements the first level of protection in hardware. This maximizes the security of the device, and allows the reuse 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 which are loaded into the device at manufacture or in the field.

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

**INTERFACES**

**Serial Interface**
The Theseus Gold 48 has a serial interface that is compliant with the ISO 7816-3 specification which defines the characteristics of Integrated Circuit Cards commonly referred to as smart cards. Several modes are implemented that allow serial connections at 9600 to 115200 bits per second. The mapping of the pins used by the Theseus Gold 48 and the ISO specification is highlighted in the following table.

**Pin Definitions**

| | Assignment Symbol | ISO 7816-3 card | Theseus Gold 48 |
|---|---|---|---|
| Supply voltage | Vcc | C1 | Vcc |
| Reset signal | RST | C2 | RST |
| Clock signal | CLK | C3 | CLK |
| Reserved | RFU | C4 | - |
| Ground | GND | C5 | GND |
| Programming Voltage | Vpp | C6 | - |
| Data input/output | I/O | C7 | I/O |
| Reserved | RFU | C8 | - |

## FEATURES

### Clocks

The Theseus Gold 48 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. This can be set to extend battery life in hand-held applications where slow interfaces are involved.

### Random Number Generator

The on-chip random number generator is compliant with the FIPS 140-1 standard, providing a rapid stream of random numbers. This allows use of the random numbers generated beyond just the provision of numbers for randomizing transmissions.

### Testability

The Theseus Gold 48 has extensive built in self-test, which allows rapid post manufacture verification of the integrity of the device. This minimizes the chances of field failures due to the card manufacturing process.

### Memory Management Unit

The Theseus Gold family gives the operating system software access to a Memory Management Unit (MMU). The MMU allows the operating system to store applications in a guarded area of memory, preventing the stored application from accessing certain chip features. This allows the operating system to download applications Over-The-Air and provide a secure area for those applications to run.

## SECURITY FEATURES

### Anti-tampering.

The Theseus Gold 48 has extensive anti-tampering features. These include monitoring the connection 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. This maximizes the endurance of the device, and provides a simple and reliable anti-tampering feedback mechanism.

### On chip Oscillator

The on-chip oscillator allows an independent clock to be generated within the chip, which isolates internal operations from the external clock signal. The internal clock frequency can be set at any time, which provides excellent protection against DPA and other attacks which monitor current use against the clock signal.

### Non-Volatile Memory Technology

The Theseus Gold Family uses a non-volatile memory technology known as Flash. This silicon technology has inherent physical security that prevents reverse-engineering and optical analysis. Flash technology is a state-of-the-art storage medium, which makes any threat to security more expensive and more difficult to implement than previous technologies.

## 3 Technical Specifications

Environment

- Single 3.0v to 5v supply ± 10%
- -20 to +80 $^0$C operating temp
- Max supply current 10 mA
- > 2 Kv ESD Protection

CPU

- Software compatible CMOS 8051 industry standard
- High speed non-standard architecture
- Traps for illegal op codes
- Standby and selectable power-down modes
- Internal Oscillator speed from 2.5 MHz to 20 MHz programmable

Memory Control

- Hardware Memory / Security Management
- Application Secure OS partitioning
- EEPROM Erase write control and verification logic

I/O

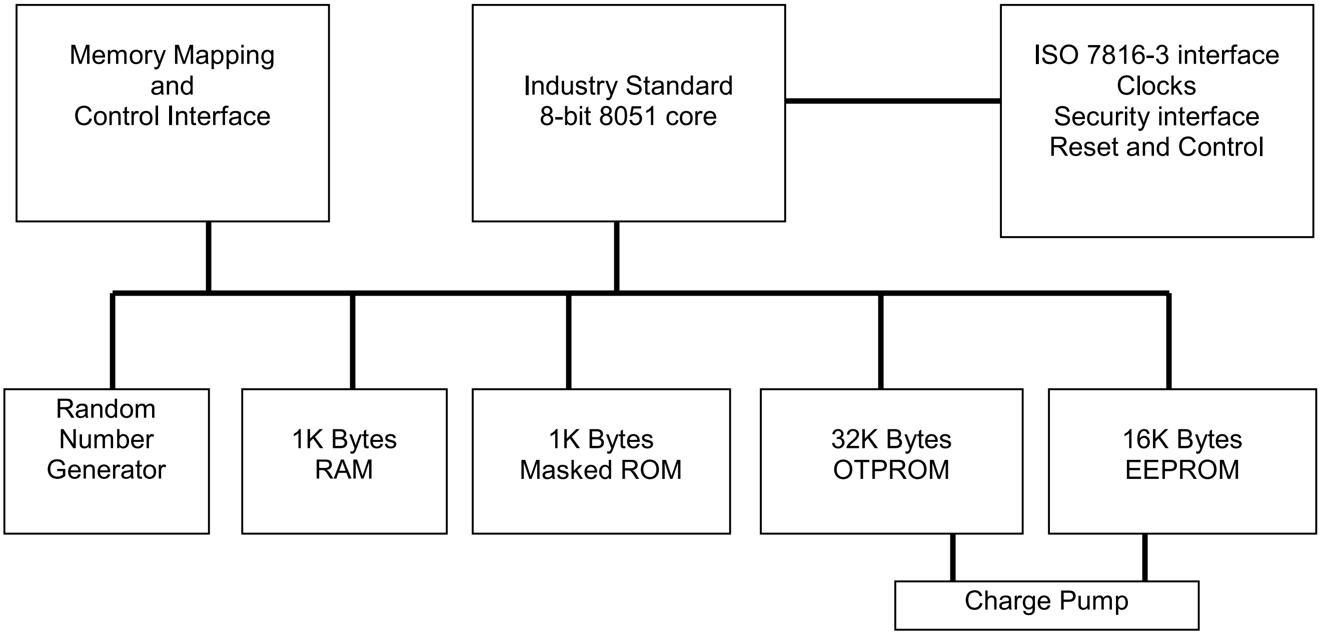
- ISO 7816-3 compliant electrical interface
- ISO 7816-3 compliant reset and response T=0 T=1 protocols

Security

- Out of frequency, out of voltage detection
- Unique chip identification number
- Notification of tampering
- Hardware Random Number Generator
- Internal clock generation

Memory

- 32K OTPROM
- 1K ROM
- 16K EEPROM
    - 10 year data retention
    - >100k read write cycles
- 1024 bytes RAM


Memory Mapping and Control Interface

Industry Standard 8-bit 8051 core

ISO 7816-3 interface
Clocks
Security interface
Reset and Control

Random Number Generator

1K Bytes RAM

1K Bytes Masked ROM

32K Bytes OTPROM

16K Bytes EEPROM

Charge Pump

# 4 Ordering Information

Please use the following codes when ordering.

Theseus Gold 48 integrated circuits:

| | |
|---|---|
| Per die, in 6" wafer, standard wafer thickness, un-sawn | TG48 - P |
| Per die, in 6" wafer, thinned to 180 µm +/- 10% thickness | TG48 - T |

Minimum quantity order of 20,000 units for wafers.

| | |
|---|---|
| Per die, in 8-contact module on reel of 35 mm tape | TG48 - M |

Minimum quantity order of 10,000 units for wafers.

| | |
|---|---|
| Per die, embedded in ISO-7816 compliant blank white cards | TG48 - CA |

Theseus Gold 48 cards are only available in sample quantities of 100 units.

Emosyn LLC makes no warranty for the use of it's products, other than those expressly contained in the Standard Terms and Conditions of Sale, which are available from the company web site. Emosyn assumes no responsibility for any errors that may appear in this document. Emosyn reserves the right to change devices and specifications 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 Emosyn or ATMI, Inc. are granted by the company in connection with the sale of Emosyn products, expressly or by implication. Emosyn's products are not authorized for use as critical components in life support devices or systems.