Theseus® Titanium 80 Datasheet

Notice

At the time of publication, this document reflects the latest features in Emosyn's offering. However, as we are continually enhancing our products, we recommend that you obtain the latest version of this document from your Emosyn representative before finalizing a design. Information in this document is subject to change without notice.

Additional Information

For additional information including, terms and conditions, prices, delivery times and technology please contact your local Emosyn representative.

Theseus Titanium 80 Summary

Emosyn's Theseus®[1] Titanium 80 is a high security, high performance Integrated Circuit (IC) designed for use within smart card applications. Theseus Titanium 80 is a secure System-On-Chip (SOC) with embedded Flash memory. Using an ISO 7816-3 serial interface, this device can communicate according to smart card industry standards. The device uses an enhanced 8051-compatible microprocessor surrounded by appropriate memory types (RAM, Flash Non-Volatile Memory). Theseus Titanium 80 also incorporates several security features designed to prohibit illegal access to user code and prevent environmental attacks.

Theseus Titanium 80 uses the latest Complementary Metal-Oxide Semiconductor (CMOS) technology and Flash Non-Volatile Memory (Flash NVM) technology. Emosyn chose the CMOS and underlying Flash NVM to meet the stringent electrical power, physical size, communication speed, and security requirements of the smart card market.

The Flash NVM is designed to operate as User Configurable Memory™[2] (UCM). UCM has all the standard characteristics of EEPROM, which are that it can be programmed, erased, and programmed again. The UCM can be configured to operate as large page EEPROM, as masked ROM, or as special Execute Only memory. The security of the Theseus Titanium 80 and the entire Theseus family of devices make them particularly suitable for areas of sensitive data.

Furthermore, the Theseus Titanium 80 offers programmable software options and features that maximize the amount of available applications and allow flexibility across the entire Theseus family of products. With these additional benefits the potential for maximizing reuse of code and the associated cost saving benefits can also be realised.

[1] Theseus is a registered trademark of Emosyn America Inc.

[2] User Configurable Memory is a trademark of Emosyn America Inc.

Features

- Enhanced 8051- compatible core that operates on 4-clock cycles
- ISO 7816-3 Serial interface compliant
- 1280 bytes of RAM (256 bytes internal scratchpad RAM {IRAM} + 1Kbytes external RAM)
- Software controlled Flash NVM
- Interrupts to trap security violations
- Software controlled power-saving options
- User-friendly code loading process
- Physical Memory Security Attributes
- Customer or factory transport code software loading options[3]
- Enhanced high speed NVM operations
- On-chip Random Number Generator
- On-chip 16-bit Timer/Counter

Environment

- Single 3V to 5V supply (± 10%)
- Operating temperature -25 ^{0}C to +85 ^{0}C
- Maximum Supply current:
    - <6 mA@30 MHz
    - <10 mA@60 MHz
- Low current Idle Mode
- External clock frequency range1-10 MHz
- 60 MHz Internal Oscillator with divide by 1 to 16
- 4kV ESD Protection
- ISO7816-2 compliant 8-contact module

Security

- Unique chip identification number
- Under Voltage detection
- Over Voltage detection
- Under Frequency on ISO clock detection
- Over Frequency on ISO clock detection
- Out of Temperature operations
- Ultra Violet light detection
- Glitch detection
- Low Voltage alert (Brownout)
- Security violations are detected, enabling user to configure interrupt or reset chip

Flash Non -Volatile Memories

- 80 Kbytes of Flash UCM (excluding 1K bytes of Locked System Memory)
- 80 Kbytes of large page UCM
- UCM erase selectable to 256 or 512 byte pages
- UCM can be configured by user software to operate as:
    - EEPROM (Default)
    - OTPROM
    - Execute Only
- Access to UCM controlled by physical memory security attributes
- 10 year Data retention on all Flash NVM bytes
- Flash NVM Guaranteed for 100K erase/write cycles
- 250K Erase/Write-cycles (typical) endurance on all Flash NVM bytes
- 2 ms page erase time (typical)
- 40 μs byte write time (typical)

Performance

- Enhanced 8051 offers 2.5x performance improvement over standard 8051
- 60 MHz capable core
- Dual data pointers speed up table handling
- Dynamic clock sources switching
- Fast UCM code loading
- Memory can be written byte-by-byte at very high speeds

[3] For further details of this option please contact your Emosyn representative.

Development Environment

- Supported by Rania®[4] Simulator Rapid Development Environment
- Programmable through Rania SwiftSIM®[5] Programmer
- Code compatible with the Keil® compiler
- Compatible development and implementation software tools

Supported Standards

- ETSI GSM 11.11
- ETSI GSM 11.12
- ISO 7816-3 compliant electrical interface
- ISO 7816-3 compliant reset and response protocols

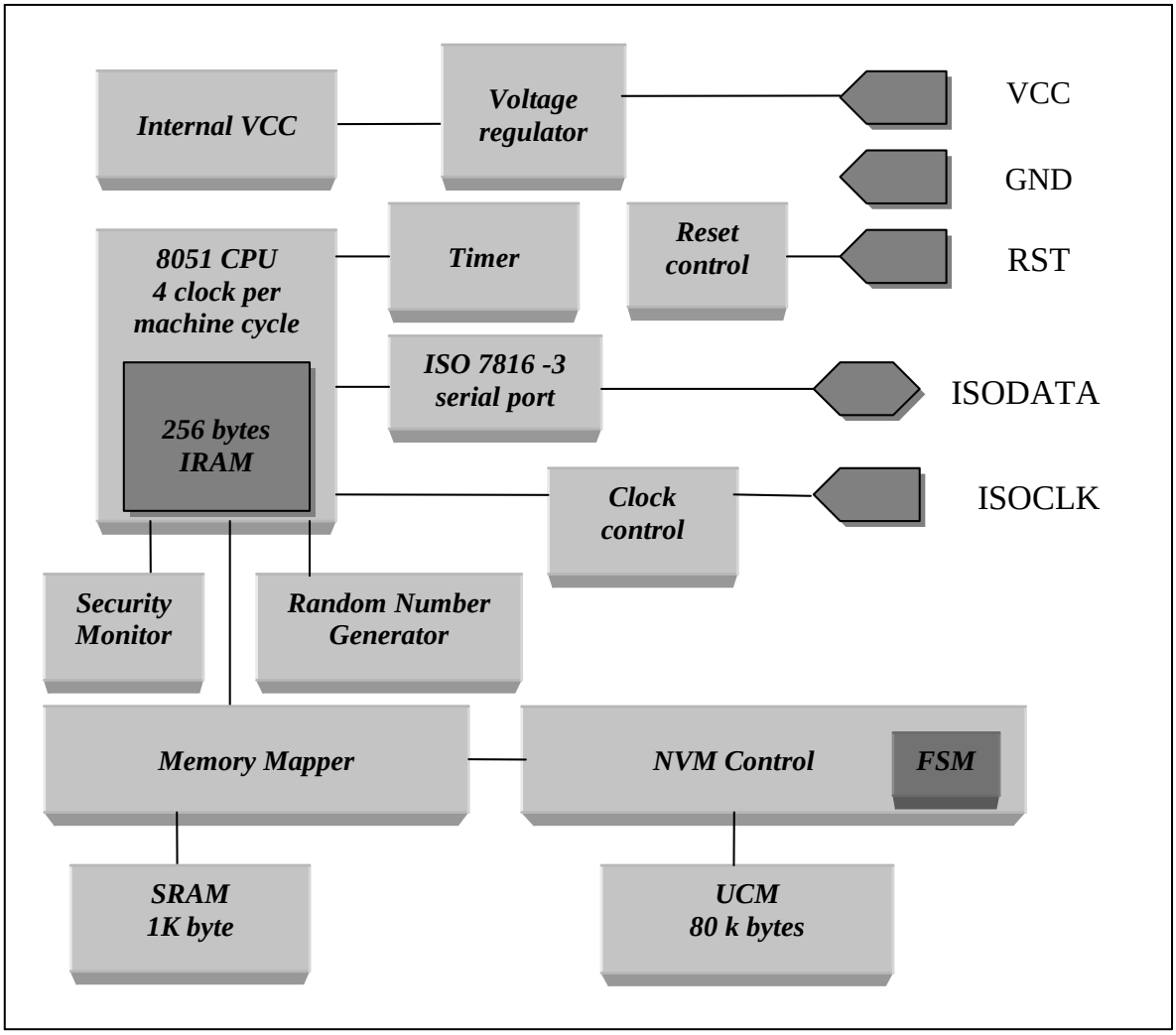
Support

- Application Notes and API Code

Document References

- Chip and Module delivery specifications (including packaging description)
- Module Qualification report

[4] Rania is a registered trademark of Emosyn America Inc.
[5] SwiftSIM is a registered trademark of Emosyn America Inc.



Interfaces

The Theseus Titanium 80 serial port is ISO 7816-3 compliant and interfaced through a control register compatible with the Theseus family of products.

The Theseus Titanium 80 utilizes an 8-pad module, designated in the following table:

Function	Assignment Symbol	Theseus Titanium 80
Supply Voltage	Vcc	Vcc
Reset Signal	RST	RST
Clock Signal	CLK	CLK
Ground	GND	GND
Programming Voltage	Vpp	-
Data Input/Output	I/O	I/O

Security Features

Each unit that passes manufacturing tests is loaded with Emosyn Transport Code for security purposes. Customers will commonly unlock the product and load their code during module embedding. Alternatively, Emosyn may provide software loading services. For additional information regarding this latter service please contact your Emosyn representative.

Note The Transport code is a small program that is pre-loaded into the User Configurable Memory (UCM). Each device will have a Transport Code, and a key to unlock the chip will be provided separate from the shipment. When the chip is powered and reset, the chip will send out an ATR, which will identify its Transport Code. If the correct key is sent to the chip, then the Transport Code program will self-erase, and prepare the chip for UCM loading. User code may then be loaded into the chip.

The Theseus Titanium 80 memory can return a unique chip identification number, which may be used in security applications. Moreover, the device has protection in Firmware against Under-voltage and Brownout-voltage operations of the device.

Anti-Tampering Features

The Theseus Titanium 80 is further protected against security attacks by multiple anti-tampering and other security features. External tampering with electrical signals or illegal software accesses to memory is monitored continuously and will cause a security condition to be registered causing processor exceptions upon detection. Using these security registers, the customer code can determine the action to take. The customer code can choose that a security exception either reset the chip, or process the software interrupt.

Non-Volatile Memory Technology Features

The Theseus family uses CMOS SuperFlash®[6] technology licensed from Silicon Storage Technology (SST) Incorporated in custom designed Non-Volatile Memory blocks. This silicon technology has inherent physical security that prevents reverse-engineering and optical analysis. SuperFlash technology is a state-of-the-art storage medium, which makes any threat to security more expensive and more difficult to implement than on previous technologies, such as Masked ROM.

[6] SuperFlash is a registered trademark of Silicon Storage Technology Inc.

Ordering information:

Please use the following codes when ordering Theseus Titanium 80 integrated circuits:

ETT80-vX.Y - Form factor

Where:

X.Y is the current version number, please see your local Emosyn representative (or your sample card) for details of the version number that your software has been written to.

Note *Emosyn products are backward compatible so that a software implementation written for Version 1.0 will run on Version 5.0 with no problems, however the converse is not necessarily true (i.e. – software written for a Version 5.1 may not run on an earlier version depending on the specific calls made). For further details or any questions please contact Emosyn Technical support.*

Form Factors include:

Die, in 8'' Wafer, thinned to 165µm +/- 10µm thickness, sawn shipped on saw frames per Emosyn Thinned Wafer Specification:

-S

8 - Contact Module on a reel of 35mm tape per Emosyn Module Specification:

-8M

Additionally, products are available with a programming service applied. The programming service (for example, ETT80-v5.0-8MP) is applied at customer option and risk. Special Terms and Conditions apply to programming. For further details please contact your local Emosyn representative.

Samples:

Samples are available in Card form, either with or without GSM punch, or in Module sample reels of 250 pieces. For further details regarding samples please contact your local Emosyn representative.