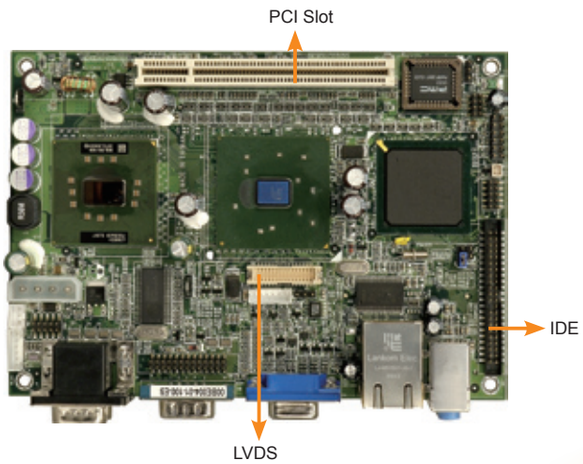
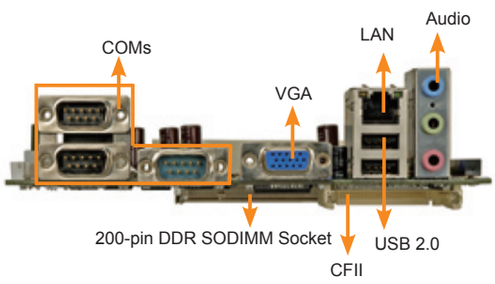
Enano-8523T

ULV Intel® Celeron® M 800MHz /1GHz Zero Cache with COM Ports, USB2.0 and TPM Security Function Support





Feature

1. Fanless EPIC embedded board
2. ULV Intel® Celeron® M 800MHz/1GHz zero cache processor
3. TPM (Trusted Platform Module) hardware security function supported
4. DDR 266MHz supports up to 1GB
5. Dual channel 18-bit LVDS independent display and CRT
6. 4 x COM ports, IDE, CFII, LAN and 4 x USB2.0

TPM Security Chip: Complete Hardware safety solution !

Feature

1. Fully compatible with TCG v1.2 Specification.
2. Sinosun 8-bits CPU Core.
3. Embedded 16KB secure data FLASH memory and 16KB RAM
4. 128KB program FLASH memory supporting online update of Firmware.
5. RSA engine supports up to 2048 bits RSA algorithm.
6. Embedded SHA-1 algorithm engine.

Specification

DDR266

- **CPU**
  ULV Intel® Celeron® M 1GHz/800MHz zero cache processor
- **System Chipset**
  Intel® 852GM + ICH4
- **BIOS**
  AMI BIOS
- **System Memory**
  1 x 200-pin SO-DIMM DDR 266MHz up to 1GB
- **Ethernet**
  10/100Mbps Intel® 82562ET
- **I/O**
  4 x USB 2.0
  1 x LPT
  1 x CFII
  4 x RS-232
  1 x PS/2 for KB/MS
  1 x IDE
- **Expansion**
  1 x PCI
- **Super I/O**
  ITE IT8712F-A
- **Audio**
  AC'97 Codec Realtek ALC655
- **Display**
  CRT integrated in Intel® 852GM
  LVDS
  Dual channel 18-bit LCD integrated in Intel® 852GM
  Support independent dual display
- **Watchdog Timer**
  Software programable supports 1-255 sec. system reset
- **Power Supply**
  +5V± 5%, 12V ±5%, 5VSB ATX power support
- **Power Consumption**
  +5V@3.66A; +12V@20mA
  (ULV Intel® Celeron® M 800 zero Cache with DDR 266MHz, 256MB RAM)
- **Temperature**
  Operation: 0 ~ 60° C (32 ~ 140° F)
- **Humidity**
  Operation: 5% ~ 95%, non-condensing
- **Dimension**
  115 mm x 165 mm
- **Weight**
  GW: 1100 g; NW: 950 g

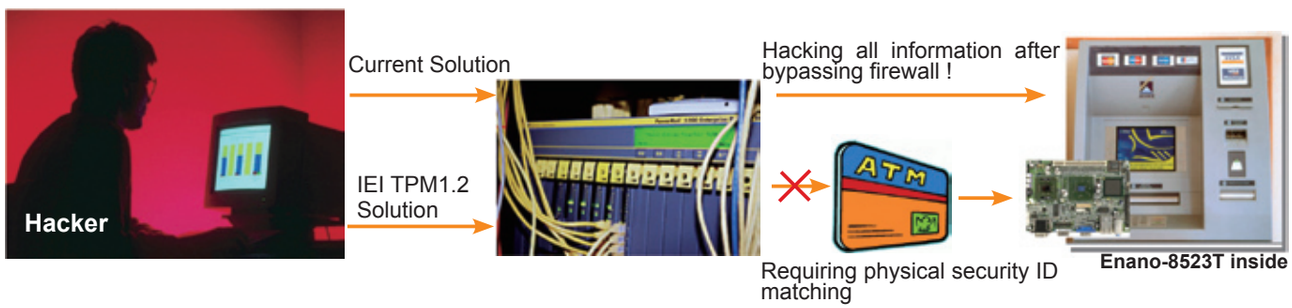
Why use a TPM v1.2?

The NANO-8523T provides the hardware security with the most cost-effective solution to build up the best value system for financial banking, healthcare environment or military applications. Hackers will never get data though network. All operations will keep records for tracking.

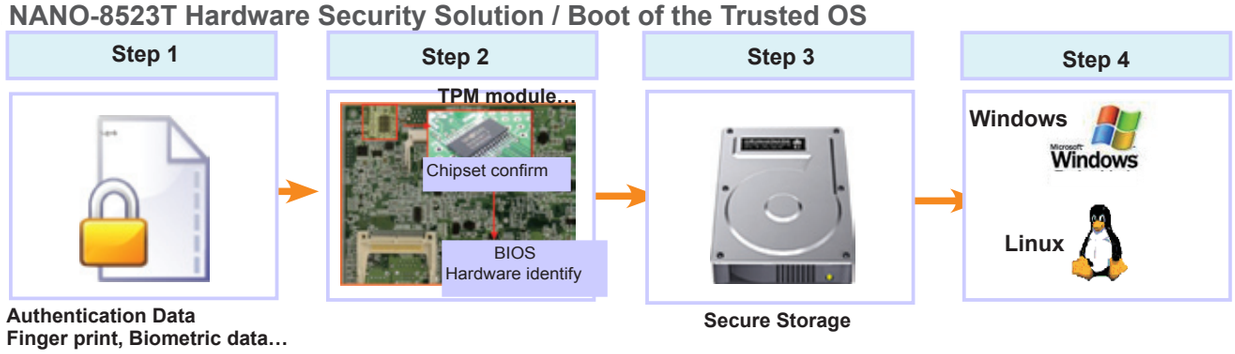
I. The Advantage of Hardware Security

Benefit: No ways for hackers to perform a remote transaction unless the hacker is physically inside the bank.

	Current Solutions	Weaknesses	IEI TPM v1.2 Solutions
Threats	Data Encryption (EFS, VPN, Encrypted email, etc.)	Encryption keys stored on hard disk are susceptible to tampering	Protected storage of keys through hardware
Unauthorized Access	- Username/ Password - Biometrics & External tokens for user authentication - Windows network logon	- Subject to dictionary attacks - Biometrics can be spoofed - Authentication credentials not bound to platform - Can be bypassed	- Protection of authentication credentials by binding them to platform - Hardware protection of authentication data



II. NANO-8523T Hardware Security Solution / Boot of the Trusted OS



Working Concepts

- During boot the TPM v1.2 gathers measurements about the running environment
- To measure == perform hash, log and extend appropriate register
- What can be measured?
  BIOS, Loader, Trusted OS, Applications
- Collected PCRs values are later used for Sealed Storage & Attestation
- TPM v1.2 only measures the running environment
  - Remote entity can decide whether to trust the running platform based on the PCR values
  - Secrets are sealed to a particular state of the platform using these measurements

Benefit

Only verified authentication data can activate system ! The most secure system control now!

Packing List

1 x Enano-8523 Single Board Computer	1 x Mini Jumper Pack
1 x PS/2 KB/MS Cable (P/N: 32000-023800-RS)	1 x Utility CD
1 x IDE Flat Cable 44p/44p (P/N: 32200-000009-RS)	1 x QIG (Quick Installation Guide)

Ordering Information

Part No.	Description
Enano-8523-1GZ-R10	EPIC SBC with ULV Intel® Celeron® M 1GHz Zero Cache CPU, LCD/CRT VGA, LAN, USB2.0, Audio and COM
Enano-8523-800Z-R10	EPIC SBC with ULV Intel® Celeron® M 800MHz Zero Cache CPU, LCD/CRT VGA, LAN, USB2.0, Audio and COM
Enano-8523T-1GZ-R10	EPIC SBC with ULV Intel® Celeron® M 1GHz Zero Cache CPU, LCD/CRT VGA, LAN, USB2.0, Audio, COM and TPM v1.2 Function
Enano-8523T-800Z-R10	EPIC SBC with ULV Intel® Celeron® M 800MHz Zero Cache CPU, LCD/CRT VGA, LAN, USB2.0, Audio, COM and TPM v1.2 Function
32200-015100-RS	LPT Cable
32100-052100-RS	ATX Power Cable