





IEI Trusted Platform Module (TPM) Solution

Hardware base security solution for data protection and reliable authentication via TPM that stores key, passwords and digital certificates.

H/W Features Comparison

| Solution | INFINEON SLB9635 TT1.2 | WINBOND WPCT200 |
|---------------------------|---|--|
| Features |  |  |
| Secure Startup | Root of Trust Measurement of early boot devices | - |
| Anti H/W Attack | Sensors and active shield | - |
| TSS API support | MS-CAPI / PKCS#11, #12 | MS-CAPI |
| H/W Certification |  | - |
| Management Tool Function | <ol style="list-style-type: none"> 1. TPM Management 2. File&Folder En/De-cryption 3. Personal Secure Drive 4. Secure E-Mail 5. Key Transferring 6. Security Policy Configuration | <ol style="list-style-type: none"> 1. TPM Owner Management 2. Password Management 3. Fingerprint Biometrics Support 4. Secure Login 5. TPM Key Backup |
| Market Segment | Complete TPM1.2 Function | Easy, Simple TPM Solution |
| TCG Specification | TCG 1.2 Compliance Trusted Platform Module | |
| Interface | Low Pin Count | |
| Software Structure | TCG Software Stack 1.2 Complaint | |
| Cryptographic Accelerator | HAS-1/ RSA algorithm | |

Pin Assignment



| Pin | Signal | Pin | Signal |
|-----|---------|-----|---------|
| 1 | LCLK | 2 | VSS |
| 3 | LFRAME# | 4 | KEYWAY |
| 5 | LRST# | 6 | VCC5 |
| 7 | LAD3# | 8 | LAD2# |
| 9 | VCC3 | 10 | LAD1# |
| 11 | LAD0# | 12 | VSS |
| 13 | SCL | 14 | SDA |
| 15 | SPDA1 | 16 | SPDA0 |
| 17 | VSS | 18 | SERIRQ |
| 19 | RC# | 20 | A20GATE |

What is EAL?

* EAL (Evaluation Assurance Level, EAL1 through EAL7) is a numerical grade assigned following the completion of a Common Criteria security evaluation, an international standard. To achieve a particular EAL, it must meet specific assurance requirements.

TPM OS Supported List

| OS Supported | Infineon | Winbond |
|--------------|----------------------------------|----------------------------------|
| Windows® | Windows® XP SP2 | Windows® XP SP2 |
| Linux | Fedora 6 (Kernel 2.6.8 or above) | Fedora 6 (Kernel 2.6.8 or above) |

IEI SBC solution with TPM support list

| Model Name | Form Factor | Chipset | TPM Type |
|-------------------------|-------------|-------------------------|---------------------|
| SPCIE-3600AM2 | PICMG 1.3 | NVIDA MCP55Pro | INFINEON WINBOND |
| PCIE-Q350 | PICMG 1.3 | Intel® Q35 + ICH9DO | |
| PCIE-9652 | PICMG 1.3 | Intel® GME965 + ICH8M-E | |
| PCIE-9152 | PICMG 1.3 | Intel® 915GM + ICH6 | |
| PCIE-690AM2/PCIE-690S1 | PICMG 1.3 | AMD® 690G + SB600 | |
| WSB-Q354 | PICMG 1.0 | Intel® Q35 + ICH9DO | |
| WSB-9452 | PICMG 1.0 | Intel® 945GM + ICH7M | |
| IMBA-X9654/IMBA-9654 | ATX | Intel® Q965 + ICH8DO | |
| IMBA-9454/IMBA-9454ISA | ATX | Intel® 945G+ ICH7 | |
| IMB-Q354 | MicroATX | Intel® Q35 + ICH9DO | |
| IMB-9454 | MicroATX | Intel® 945G+ ICH7 | |
| IMB-9452 | MicroATX | Intel® 945GM + ICH7M | |
| KINO-9652 | Mini-ITX | Intel® G M965 + ICH8M | |
| KINO-9454 | Mini-ITX | Intel® 945G+ ICH7 | |
| KINO-690AM2 /KINO-690S1 | Mini-ITX | AMD® 690G + SB600 | |
| NOVA-945GSE | 5.25" | Intel® 945GSE + ICH7M | WINBOND |

Ordering Information

| Model Name | Description |
|--------------|--|
| TPM-IN01-R10 | INFINEON 20 pin Trusted Platform Module with S/W Management Tool |
| TPM-WI01-R10 | WINBOND 20 pin Trusted Platform Module with S/W Management Tool |