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 / Features	INFINEON SLB9635 TT1.2	SINOSUN SSX35BCB	WINBOND WPCT200
			
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	MS-CAPI
H/W Certification	EAL 4	EAL 3	-
Management Tool Function	1. TPM Management 2. File&Folder En/De-cryption 3. Personal Secure Drive 4. Secure E-Mail 5. Key Transferring 6. Security Policy Configuration	1. TPM Management 2. File&Folder En/De-cryption 3. Virtual Encrypted Disk 3. Password Management	1. TPM Management 2. Windows Password Login
Market Segment	Complete TPM1.2 Function	China Market Approved by the China Data Security Dept	Easy, Simple TPM Solution
TCG Specification	TCG 1.2 Compliance Trusted Platform Module		
Interface	Low Pin Count		
Software Structure	TCG Software Stack 1.2 Compliant		
Cryptographic Accelerator	HAS-1/ RSA algorithm		

Pin Assignment

Pin	Singnal	Pin	Singnal
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.

SBC solution with TPM support list

Model Name	Form Factor	Chipset	TPM Type	BIOS
PCIE-9152	PICMG 1.3	Intel 915GM + ICH6	SINOSUN INFINEON WINBOND 20-pin Module for Customer Option	AMI (TPM modules requires to combine with BIOS Setting)
WSB-9452	PICMG 1.0	Intel 945GM + ICH7M		
IMBA-X9654	ATX	Intel Q965 + ICH8DO		
IMBA-9454	ATX	Intel 945G + ICH7		
IMB-9454	micro-ATX	Intel 945G + ICH7		
IMB-9452	micro-ATX	Intel 945GM + ICH7M		
KINO-9454	Mini-ITX	Intel 945G + ICH7		
KINO-690AM2	Mini-ITX	ATI RS690 + ATI SB600		
KINO-690S1	Mini-ITX	ATI RS690 + ATI SB600		
KINO-LUKE	Mini-ITX	VIA LUKE + VIA VT8237R PLUS		
ENANO-8523T	EPIC	Intel 852GM + ICH4	On-board SINOSUN TPM	
WAFER-8522	3.5”	Intel 852GM + ICH4		

Ordering Information

Model Name	Description
TPM-IN01-R10	INFINEON 20 pin Trusted Platform Module with S/W Management Tool
TPM-SI01-R10	SINOSUN 20 pin Trusted Platform Module with S/W Management Tool
TPM-WI01-R10	WINBOND 20 pin Trusted Platform Module with S/W Management Tool