SSX35

Trusted platform module (TPM)

兆日
SINOSUN

Datasheet

April 2005
Revision 1.6

Contents

Revision History

Revision	Date	Description
Rev1.6	April 2005	4.7K resistor is provided on PP pin by liud

1. General Description

(1) Fully compatible with TCG v1.2 Specification[1].

(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.

(7) Integrated RNG for key generation and encryption transmission.

(8) LPC interface and serial interface in conformance to ISO 7816 Standard.

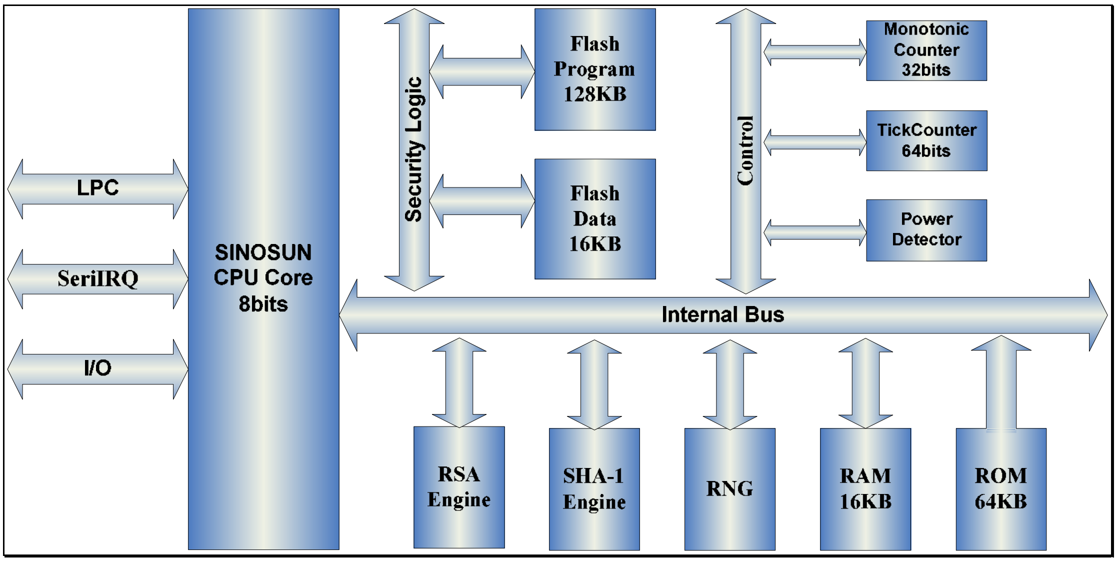


Figure 1-1 SSX35ACB structure

2. Product Parameters

(1) Supply Voltage: 3.3V ± 10%

(2) Frequency: 33MHz

(3) Program Space: 128KB FLASH memory and 64KB ROM

(4) Data Space: 16KB FLASH memory and 16KB RAM

(5) Work Current: < 30mA

(6) Idle Current: < 0.1mA

(7) Speed: RSA 2048 bits Signature (Decryption): <300ms
RSA 2048 bits Verification (Encryption): <40ms
RSA 1024 bits Signature (Decryption): <120ms
RSA 1024 bits Verification (Encryption): <15ms
SHA-1(1M bits) Computing Speed: <258ms
2048 bits RSA Key pair generation: <10 Seconds

(8) Package: TSSOP28

3. Main Functions

(1) Measure, store and report on the integrity of platform

Using SHA-1 Hash function, SSX35 can measure, store and report the platform integrity.

(2) Identity Verification

Use AIK generated inside the chip to complete digital signature of the data

(3) Encrypt and store the sensitive data

SSX35 stores the sensitive data in the shielded area of the chip, or it can encrypt the data with storage key and store them in the generic memory on the platform.

(4) Authorized access to internal info:

Access to resources (include keys, sensitive data encrypted) managed by SSX35 must be authorized by SSX35.

(5) Encrypted transmission of commands and data

While the SSX35 exchanges commands and data with external entity, it not only verifies the User's ID, but also prevents the key data of ID verification from being stolen, replayed or attacked through the communication line.

（6） Provide secure administration mechanism for trusted platform SSX35 can protect the platform from illegal remote access through physical presence.

4. Pin And Signal Overview

Pinout description as figure4-1and table 4-1

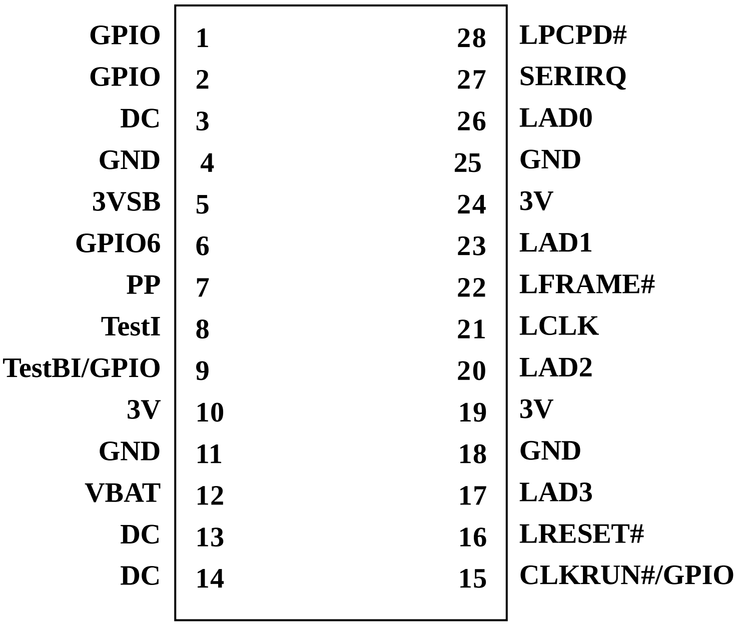


Figure 4-1 SSX35ACB pinout description

Table 4-1

Signal	Pin(s)	Type	Description
LAD[3:0]	26, 23, 20, 17	BI	**Multiplexed Command, Address and Data BUS** (see LPC Interface Spec)
LPCPD#	28	I	power down
LCLK	21	I	33MHz clock (see LPC Interface Spec).
LFRAME#	22	I	**Frame** indicates start of a new LPC cycle, termination of broken cycle (see LPC Interface Spec)
LRESET#	16	I	**System reset signal** (see LPC Interface Spec)
SERIRQ	27	BI	**Serialized IRQ** is used to handle interrupt support (see LPC Interface Spec)
CLKRUN#/GPIO	15	BI	Same as PCI CLKRUN#. Active Low. internal pull-down GPIO will default to low.
PP	7	I,BI	Physical Presence, active high, internal pull-down. Used to indicate Physical Presence to the TPM.
DC	3,13,14	I	Do not connect
GPIO	1	BI	Defaults high. (weak internal pull-up)
GPIO	2	BI	Defaults high (weak internal pull-up)
GPIO6	6	BI	GPIO Defaults high (weak internal pull-up)
TESTI	8	I	This pin will be pulled low on motherboard. Assuming: Pull high to enable Test mode. Pull low to disable Test mode and enable GPIO on pin 9(TESTBI)
TESTBI/GPIO	9	BI	TESTBI: Test port. If TESTI is pulled low acts as a GPIO. GPIO will default high(weak internal pull-up)
Power			
3V	10, 19 24	I	This is a 3.3 volt DC power. The maximum power for this interface is 250 ma.

GND	4, 11, 18, 25	I	Zero volts.
VBAT	12	I	3.3V battery input.
3VSB	5	I	3.3 volt standby DC power rail.

5. Absolute Maximum Ratings

Operating Temperature........................…………...….0°C to +70°C

Storage Temperature (without Bias)......………..….-20°C to +85°C

Voltage on I/O Pins.........................…………...-0.1 to VCC +0.3V

Voltage on VCC with Respect to Ground.…………..............6.0V

Maximum ESD Voltage.............................……….…...…......2000V

***NOTICE:** Stresses beyond those listed under “Absolute Maximum Ratings” may cause permanent damage to the device. This is a stress rating only and functional operation of the device at these or any other conditions beyond those indicated in the operational sections of this specification may cause temporary or permanent failure. Exposure to absolute maximum rating conditions for extended periods may affect device reliability.

Table 5-1**.** DC Parameters

V_{CC} = 3.0 to 3.6V; Temperature = 0 to 70°C

Symbol	**Parameter**	**Min**	**Nom**	**Max**	**Units**
VCC	Supply Voltage	3.0	3.3	3.6	V
ICC	Operating Current at fclk = 33 MHz		25	50	mA
IST	Static Current		5	10	mA
ISL	Static Standby current, reset active		40	100	µA
ILIO	Input Leakage		0.1	3	µA
VIH	Input High voltage	1.5		3.6	V
VIL	Input Low voltage	-0.5		0.8	V
VOH	Output High Voltage	0.9 * VCC	0.98 * VCC		V
VOL	Output Low Voltage			0.1 * VCC	V
IOLCR	Output Low Current	7			mA
CI	Input Pin Capacitance		6		pF

Note: These parameters guaranteed but not tested.

Table 5-2. AC Parameters

Cl = 10pf. VCC = 3.0 to 3.6V; Temperature = 0 to 70°C

Symbol	**Parameter**	**Min**	**Nom**	**Max**	**Units**
TVAL	CLK to Signal Valid Delay – LAD0-3	2	5	10	ns
TON	Float to Active Delay	2	4		ns
TOFF	Active to Float Delay			28	ns

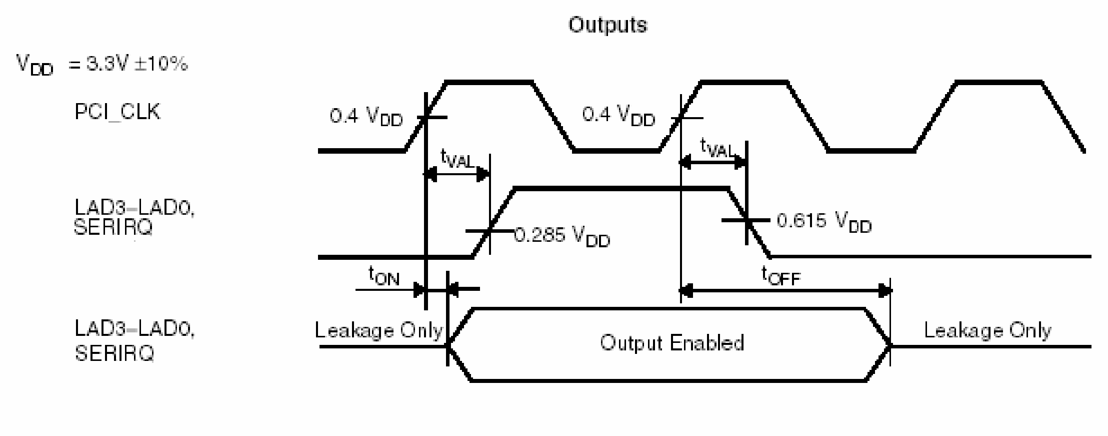


Figure 5-1 AC parameters

Table 5-3 LPC bus signal delay to PCICLK

Symbol	**Parameter**	**Min**	**Nom**	**Max**	**Units**
TSU	Input Setup Time to CLK	7			ns
TH	Input Hold Time from CLK	0			ns

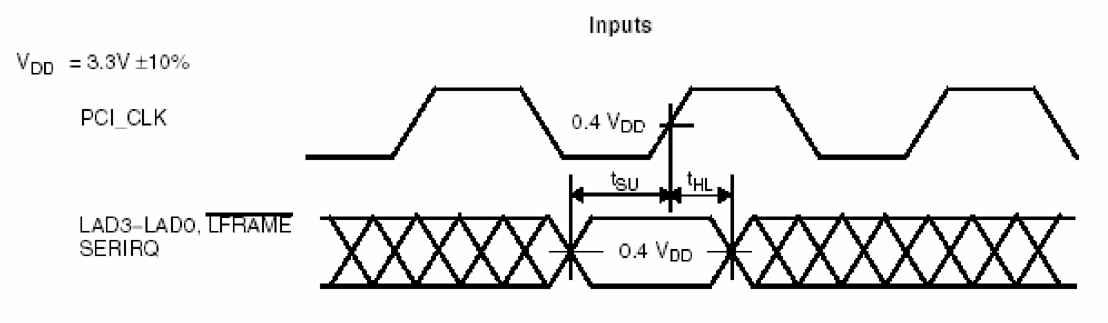


Figure 5-2 AC parameters

Table 5-4 reset signal character

Symbol	Parameter	Min	Nom	Max	Units	Notes
TRST	Reset Active Time after Power Stable	1			ms	Note 2
TRST-CLK	Reset Active after CLK Stable	100			ms	Note 2
TRST-OFF	Reset Active to Output Float Delay			40	ns	Note 2

Table 5-5 clock signal character

Symbol	Parameter	Min	Nom	Max	Units	Notes
TCYC	CLK Period	29.5	30	31	ns	Note 3
T_{LOW}	CLK Low Duration	13.4		18	ns	Note 1, Note 3
THIGH	CLK High Duration	13.4		18	ns	Note 1, Note 3

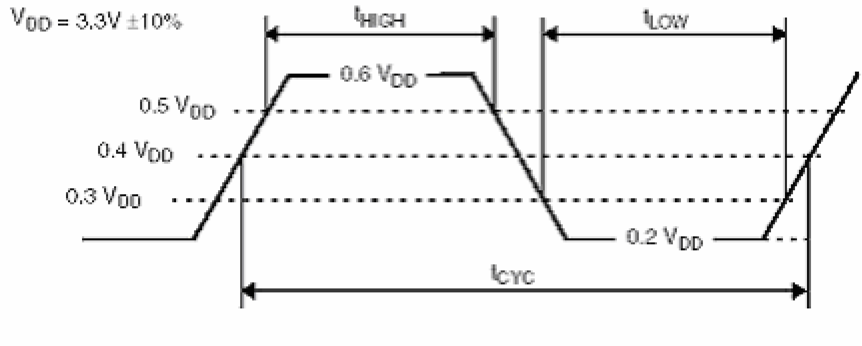


Figure 5-3 clock signal character

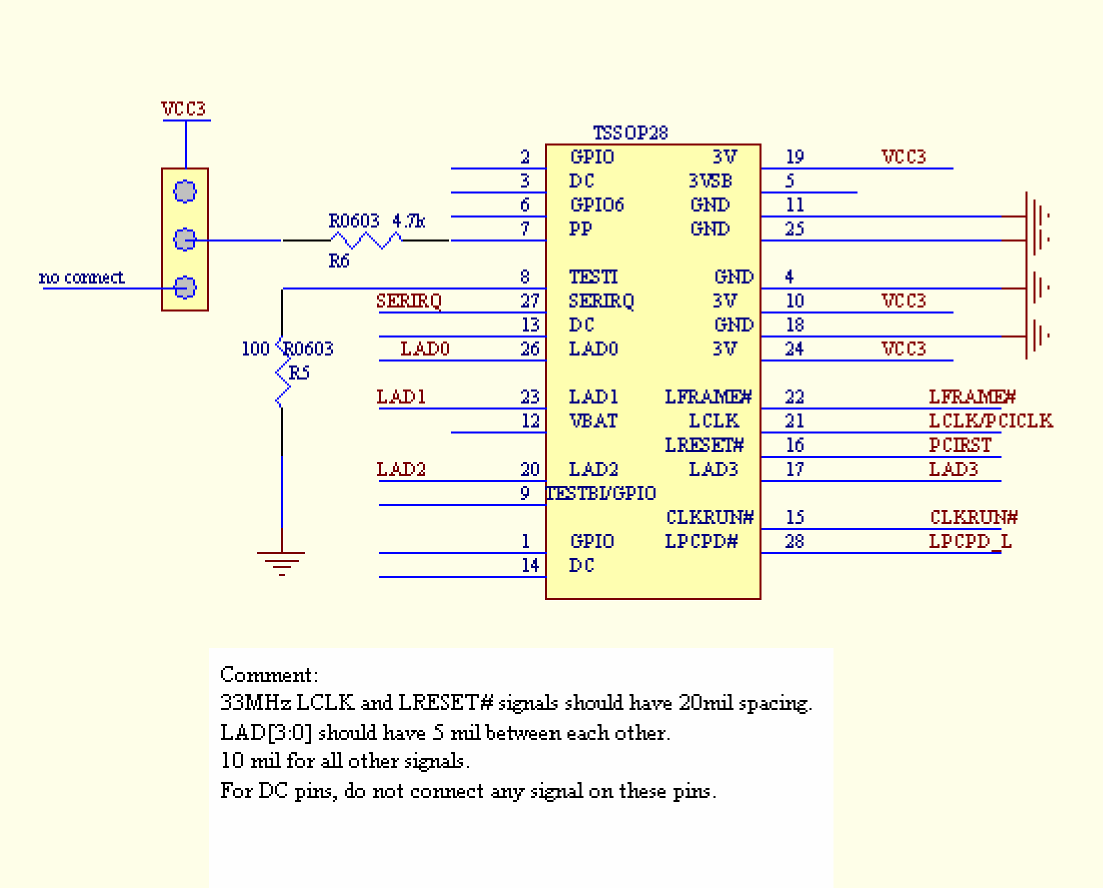
Note:

(1) All parameters measured with respect to signal crossing Vtest = 0.4 * VCC unless otherwise noted.

(2) These parameters guaranteed but not tested.

(3) The minimum parameter must never be violated under any circumstances unless Ireset# is asserted.

6. Typical Application



Comment:
33MHz LCLK and LRESET# signals should have 20mil spacing.
LAD[3:0] should have 5 mil between each other.
10 mil for all other signals.
For DC pins, do not connect any signal on these pins.

Figure 6-1 28pins typical application

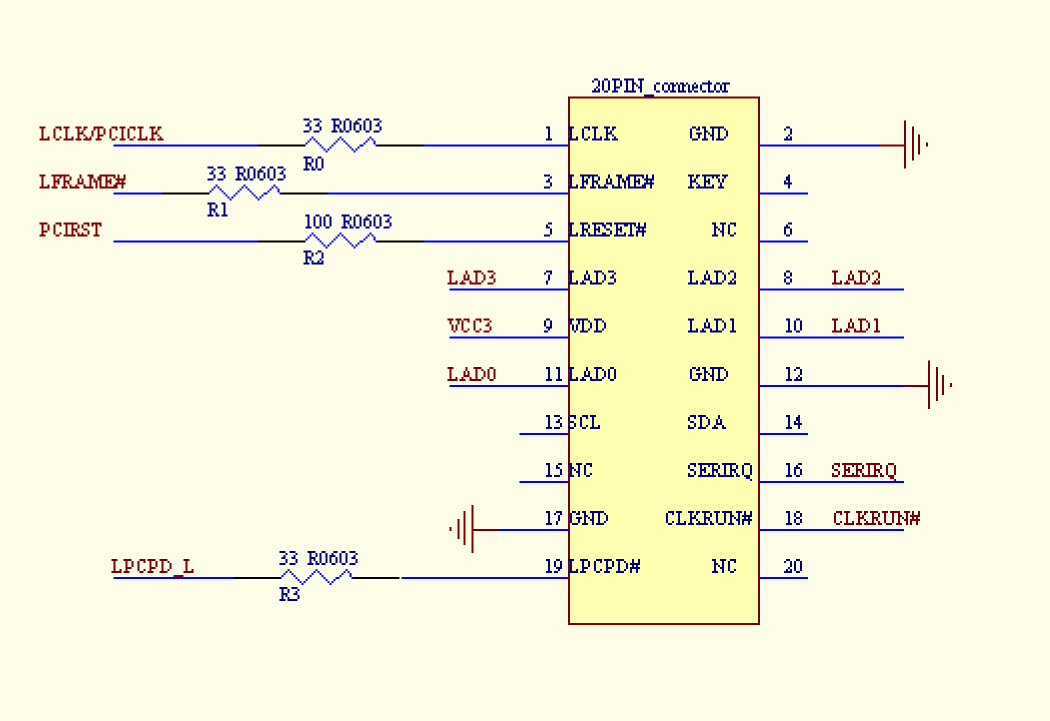


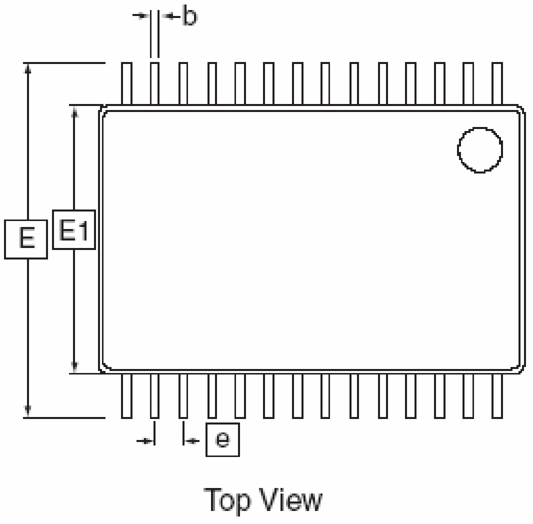
Figure 6-2 20pins connector typical application

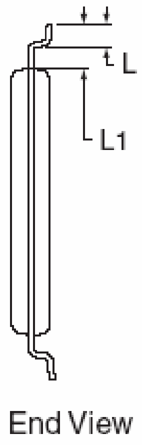
Note:

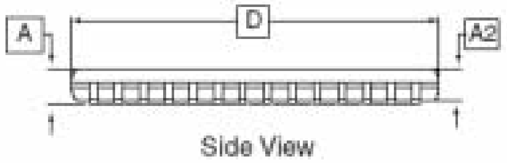
1. 33MHz LCLK and LRESET# signals should have 20mil spacing.
2. LAD[3:0] should have 5 mil between each other.10 mil for all other signals.
3. For DC pins, do not connect any signal on these pins.
4. GPIO_ON : the GPIO signal on board , For the BIOS detect PP status from it.

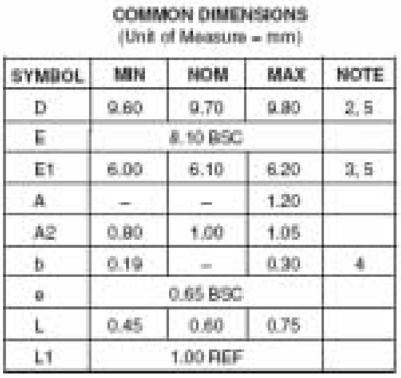
7. Package Drawing

TSSOP28 （figure 7-1）









COMMON DIMENSIONS
(Unit of Measure = mm)

SYMBOL	MIN	NOM	MAX	NOTE
D	9.60	9.70	9.80	2, 5
E	8.10 BSC			
E1	6.00	6.10	6.20	3, 5
A	–	–	1.20	
A2	0.80	1.00	1.05	
b	0.19	–	0.30	4
e	0.65 BSC			
L	0.45	0.60	0.75	
L1	1.00 REF			

Figure 7-1 package drawing

Notes:

(1) This drawing is for general information only. Please refer to JEDEC Drawing MO-153, Variation DB for additional information.

(2) Dimension D does not include mold Flash, protrusions or gate burrs. Mold Flash, protrusions and gate burrs shall not exceed 0.15 mm (0.006 in) per side.

(3) Dimension E1 does not include inter-lead Flash or protrusions. Inter-lead Flash and protrusions shall not exceed 0.25 mm (0.010 in) per side.

(4) Dimension b does not include Dambar protrusion. Allowable

Dambar protrusion shall be 0.08 mm total in excess of the b dimension at maximum material condition. Dambar cannot be located on the lower radius of the foot. Minimum space between protrusion and adjacent lead is 0.07 mm.

(5) Dimension D and E1 to be determined at Datum Plane H.

8. Chip Mark

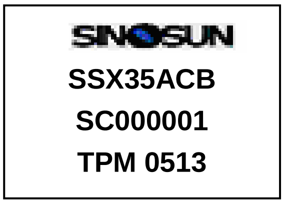


Figure 8-1 SSX35ACB chip mark

SSX35ACB is our chip name and TPM0513 is our chip’s S/N number:

[1] SSX35 is fully compatible with the commercial encryption lows and regulations in China and TCG standard.