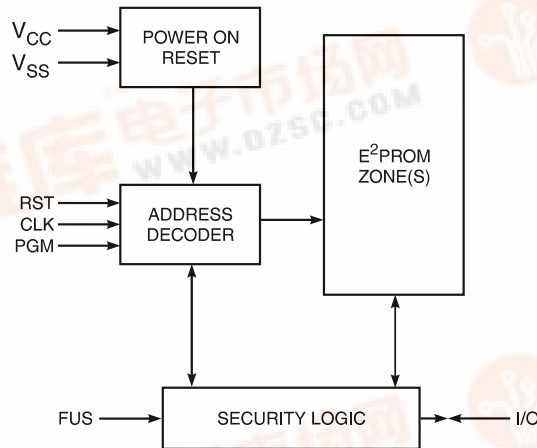


## Features

- 1K x 1 Serial E<sup>2</sup>PROM With Security Logic
- Available in Two Memory Organizations:
  - AT88SC10111K x 1Memory Zone
  - AT88SC1022512 x 1Memory Zone
- Supports ISO/IEC 7816-3 Synchronous Protocol
- Stores and Validates Security Codes
- Counts Incorrect Security Code Attempts
- Provides Transport Code Security
- Manufactured Using Low Power CMOS Technology
- VPP Internally Generated
- 2  $\mu$ s Read Access Time; 5 ms Write Cycle Time
- Temperature Range From -25°C to 70°C
- ESD Immunity > 4K Volts
- High Reliability:
  - 100,000 Write/Erase Cycles
  - 100 Years Data Retention

## Block Diagram



## Description

The AT88SC101/102 family provides 1024 bits of serial E<sup>2</sup>PROM (Electrically Erasable and Programmable Read Only Memory) with additional security logic for use in secure smart card applications. The AT88SC101 is available in one 1024 x 1 bit memory zones, and the AT88SC102 is available in two 512 x 1 bit memory zones.

## ISO Card Configuration

ISO Contact	Pad #	Pad Name	Description
C1	8	V <sub>CC</sub>	Operating Voltage
C2	7	RST	Reset
C3	6	CLK	Clock and Address Control
C4	5	FUS	Identification Fuses
C5	1	V <sub>SS</sub>	Ground
C6	2	NC	No Connect
C7	3	I/O	Bi-directional Data Port
C8	4	PGM	Programming Control

## Card Module Contacts

V <sub>CC</sub>	C1	C5	V <sub>SS</sub>
RST	C2	C6	N/C
CLK	C3	C7	I/O
FUS	C4	C8	PGM



## Smart Card ICs

## 1K E<sup>2</sup>PROM with Security Logic

## AT88SC101 AT88SC102





The security features of Atmel's AT88SC101/102 include:

- data access only after validation of the security code
- permanent invalidation of device upon four consecutive false security code presentations
- read/write protection of certain memory zones
- device reset if power drops

secure transport of devices using transport code compare sequence

The AT88SC101/102 is manufactured using low-power CMOS technology and features its own internal high-voltage pump for single voltage supply operation. The devices are guaranteed to 100,000 erase/write cycles and 100 year data retention. Endurance up to one-million

## AT88SC101 and AT88SC102 Memory Map

Memory Partitions	AT88SC101		AT88SC102	
	Address	Bits	Address	Bits
Fabrication Zone (FZ)	0 - 15	16	0 - 15	16
Issuer Zone (IZ)	16 - 79	64	16 - 79	64
Security Code (SC)	80 - 95	16	80 - 95	16
Security Code Attempts Counter (SCAC)	96 - 111	16	96 - 111	16
Code Protected Zone (CPZ)	112 - 175	64	112 - 175	64
Application Zone 1 (AZ1)	176 - 1199	1024	176 - 687	512
Application Zone 1 Erase Key (EZ1)	1200 - 1231	32	688 - 735	48
Application Zone 2 (AZ2)	—	—	736 - 1247	512
Application Zone 2 Erase Key (EZ2)	—	—	1248 - 1279	32
Erase Counter (EC)	1232 - 1359	128	1280 - 1407	128
Memory Test Zone (MTZ)	1360 - 1375	16	1408 - 1423	16
TOTAL BITS		1376		1424

## Definition of AT88SC101/102 Memory Partitions

**FABRICATION ZONE (16 bits):** Programmed by the manufacturer with a specific identifier for each customer. FUSE1 is blown by the manufacturer after programming the fabrication code, which makes the fabrication zone unalterable.

**ISSUER ZONE (64 bits):** Programmed by the issuer before finalizing personalization. The data stored in the issuer zone is unalterable after FUSE2 is blown.

**SECURITY CODE (16 bits):** Must be presented by the issuer to access circuit memory and personalize device before blowing FUSE2. This secures transportation between the manufacturer and the issuer. After the device is personalized and FUSE2 is blown, this code protects the access to the application zone(s) of the card.

**SECURITY CODE ATTEMPTS COUNTER (16 bits):** Counts the number of incorrect security code attempts. The device is locked after 4 false presentations.

**USER PROTECTED ZONE (64 bits):** Writing and erasing this zone is protected. The number of program/erase cycles is guaranteed up to 100,000.

**APPLICATION ZONE(S) (1024 or 512 bits):** Reading and programming the application zone(s) are controlled by the first 2 bits of the zone (PR, RD) and by the security code (Tables 1 and 2). The erasure of each zone is protected by an erase key specific to each zone.

**APPLICATION ZONE ERASE KEY (32 or 48 bits):** Must be presented to authorize the erasure of the application zone(s). The key(s) must be programmed during the personalization of the circuit.

**ERASE COUNTER (128 bits):** Limits the number of erasures of the last zone to 128 or less.

**MEMORY TEST ZONE (16 bits):** Allows pattern testing at this memory location.

## Memory Access to AT88SC101 and AT88SC102

The access to the memory is controlled by the state of the internal fuses and by the voltage supply applied on the FUS pad:

FUS Pad Voltage	State of the FUSES FUSE 1 FUSE 2		Access Conditions See:
0V	Either	Either	Table 2
5V	Blown	Not Blown	Table 1
5V	Blown	Blown	Table 2

**Table 1. AT88SC101/102 Access Conditions During Personalization (FUSE 2 Not Blown)**

Zones	S C	1 P R	1 R D	2 P R	2 R D	E Z 1	E Z 2	E C	READ	WRITE 1 (Erase)	WRITE 0 (PROG)	Compare
FZ	X	X	X	X	X	X	X	X	YES	NO	NO	NO
IZ	0	X	X	X	X	X	X	X	YES	NO	NO	NO
	1	X	X	X	X	X	X	X	YES	YES	YES	NO
SC	0	X	X	X	X	X	X	X	NO	NO	NO	YES
	1	X	X	X	X	X	X	X	YES	YES	YES	NO
SCAC	0	X	X	X	X	X	X	X	YES	NO	YES	NO
	1	X	X	X	X	X	X	X	YES	YES	YES	NO
CPZ	0	X	X	X	X	X	X	X	YES	NO	NO	NO
	1	X	X	X	X	X	X	X	YES	YES	YES	NO
AZ1	0	X	0	X	X	X	X	X	NO	NO	NO	NO
	0	X	1	X	X	X	X	X	YES	NO	NO	NO
	1	X	X	X	X	X	X	X	YES	YES	YES	NO
EZ1	0	X	X	X	X	X	X	X	NO	NO	NO	NO
	1	X	X	X	X	X	X	X	YES	YES	YES	NO
AZ2	0	X	X	X	0	X	X	X	NO	NO	NO	NO
	0	X	X	X	1	X	X	X	YES	NO	NO	NO
	1	X	X	X	X	X	X	X	YES	YES	YES	NO
EZ2	0	X	X	X	X	X	X	X	NO	NO	NO	NO
	1	X	X	X	X	X	X	X	YES	YES	YES	NO
EC	0	X	X	X	X	X	X	X	YES	NO	YES	NO
	1	X	X	X	X	X	X	X	YES	YES	YES	NO
MTZ	X	X	X	X	X	X	X	X	YES	YES	YES	NO

Notes: SC:SC = 1 after validation of security code  
 1PR:1st bit of AZ1 (Bit 176)  
 1RD:2nd bit of AZ1(Bit 177)  
 2PR:1st bit of AZ2 (Bit 736) - AT88SC102 only

2RD: 2nd bit of AZ2 (Bit 737) - AT88SC102 only  
 EZ1: EZ1 = 1 after a valid presentation of erase key 1  
 EZ2: EZ2 = 1 after a valid presentation of erase key 2  
 EC: EC = 1 when the counter is not empty.



**Table 2. AT88SC101/102 Access Conditions After Personalization (FUSE 2 Blown)**






Zones	S C	1 P	1 R	2 P	2 R	E Z	E Z	E C	READ	WRITE 1 (Erase)	WRITE 0 (PROG)	Compare
		R	D	R	D	1	2					
FZ	X	X	X	X	X	X	X	X	YES	NO	NO	NO
IZ	X	X	X	X	X	X	X	X	YES	NO	NO	NO
SC	0 1	X X	X X	X X	X X	X X	X X	X X	NO NO	NO YES	NO YES	YES NO
SCAC	0 1	X X	X X	X X	X X	X X	X X	X X	YES YES	NO YES	YES YES	NO NO
CPZ	0 1	X X	X X	X X	X X	X X	X X	X X	YES YES	NO YES	NO YES	NO NO
AZ1	0 0 1 1 1 1	X X 0 0 1 1	0 1 X X X X	X X X X X X	X X X X X X	X X 0 1 0 1	X X X X X X	X X X X X X	NO YES YES YES YES YES	NO NO NO YES NO YES	NO NO NO NO YES YES	NO NO NO NO NO NO
EZ1	X	X	X	X	X	X	X	X	NO	NO	NO	YES
AZ2	0 0 1 1 1 1 1 1 1	X X X X X X X X X	X X X X X X X X X	X X 0 0 0 1 1 1 1	X X X X X X X X X	X X X X X X X X X	X X 0 X X X X X X	X X X X X X X X X	NO YES YES YES YES YES YES YES YES	NO NO NO NO YES NO NO NO YES	NO NO NO NO NO YES YES YES YES	NO NO NO NO NO NO NO NO NO
EZ2	X	X	X	X	X	X	X	X	NO	NO	NO	YES
EC	X	X	X	X	X	X	X	X	YES	NO	YES	NO
MTZ	X	X	X	X	X	X	X	X	YES	YES	YES	NO

Notes: SC:SC = 1 after validation of security code  
 1PR:1st bit of AZ1 (Bit 176)  
 1RD:2nd bit of AZ1(Bit 177)  
 2PR:1st bit of AZ2 (Bit 736) - AT88SC102 only

2RD: 2nd bit of AZ2 (Bit 737) - AT88SC102 only  
 EZ1: EZ1 = 1 after a valid presentation of erase key 1  
 EZ2: EZ2 = 1 after a valid presentation of erase key 2  
 EC: EC = 1 when the counter is not empty.

## Modes of Operation

The AT88SC101/102 has four operation modes selected by PGM, RST, CLK, and by the internal counter:

Inputs Micro Instructions	PGM	RST	CLK	Definitions
RESET	X		0	The address counter is reset to 0 and the first bit of the memory is available on I/O after the falling edge of RST and CLK hit 0. Note: The INC instruction is disabled when RST is high (Figure 1). Address counter is reset on the falling edge of RESET.
INC (INC/READ)	0	0		The address counter is incremented and the first bit is available on I/O after the falling edge of the clock (unless reading is forbidden) (Figure 2). Address increments on falling edge of CLK. Data is released after the falling edge of CLK.
CMP (INC/CMP)	0	0		Comparison of the bit presented to the card to the internal bit of the memory (for secret codes only). The bit should stay stable on I/O during the time CLK is low. The address counter is incremented on the falling edge of the CLK (Figure 3).
WRITE	1	0		I/O must be positioned on 0 for programming or on 1 for erasure before the rising edge of CLK which must stay on 1 for at least 5ms. The bit addressed (which will be written) is available on I/O after the falling edge of the CLK (Figure 4).
VERIFY	0	0		

Notes: 1. Output is disabled (Hi state) on addresses where read is disabled.

2. If  $V_{DD}$  falls between approximately 3V and 4V the chip will execute a power-on reset.

3. The 2 instructions CMP and UP are coded (0,0) on CLK and PGM. The circuit will distinguish between the 2 instructions by testing the internal address counter (CMP can only be done with the addresses corresponding to the security code or erase key).

4. The internal address counter counts up to 1519 for 101 and 1567 for 102. An additional INC sets the counter to 0.

**Table 5. AT88SC101/102 Micro Instructions**

Instruction	Bit	Word	Application Zone	Global (When Fuse 2 = 1)
READ	RESET n INC; position counter on bit	—	—	—
WRITE ( WRITE 0)	RESET n INC; position counter on bit WRITE0 INC; go to next bit WRITE0;...	—	—	RESET n INC; n = 1392 (101) n = 1440 (102) WRITE 0
ERASE (WRITE 1)	—	RESET n INC; position counter on first bit in word WRITE 1 n INC; position counter on first bit in next word WRITE 1...	verify erase keys <u>AT88SC101 Zone 1/88SC102 Zone 2:</u> RESET 32 CMP n INC; n = 1232 (101), n = 1280 (102) VERIFY 1; verify 1 in EC WRITE 0; write 0 in EC WRITE 1; erase application zone  <u>AT88SC102 Zone 1:</u> RESET 48 CMP n INC; n = 736 WRITE 1; erase application zone	RESET n INC; n = 1392 (101) n = 1440 (102) WRITE 1
CMP • SECURITY CODE	—	RESET 79 INC; position counter on bit preceding SC 16 CMP; verify security code n INC; If none of the 1st 4 bits of the SCAC is 1, then 4 unsuccessful attempts have been made to verify SC, and the device is inoperable. If any of the 1st 4 bits is a 1, then: WRITE 0 WRITE 1; Reset the SCAC	—	—
CMP • ERASE KEYS	—	RESET n INC; position counter on bit preceding access code or erase key n CMP; verify access code or erase key ; n = 32 or 48 bits	—	—

Figure 1. Reset

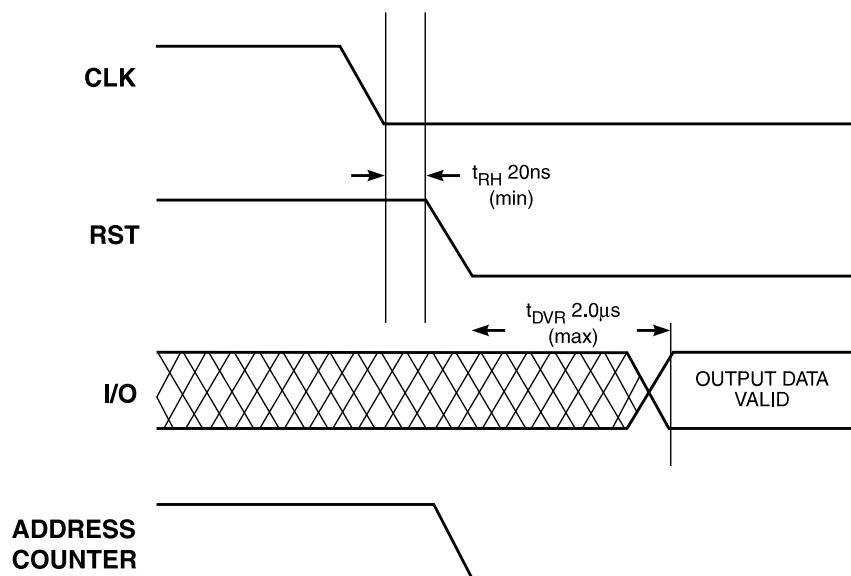
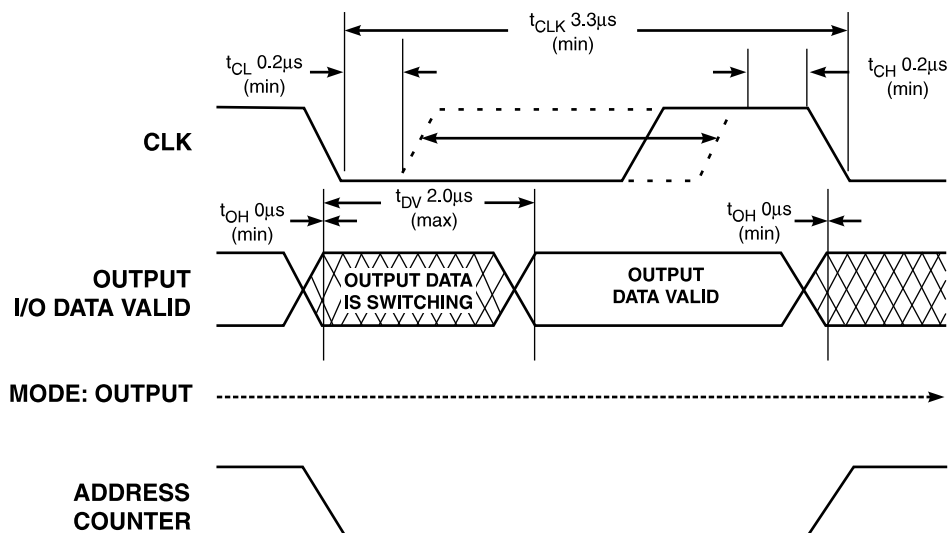
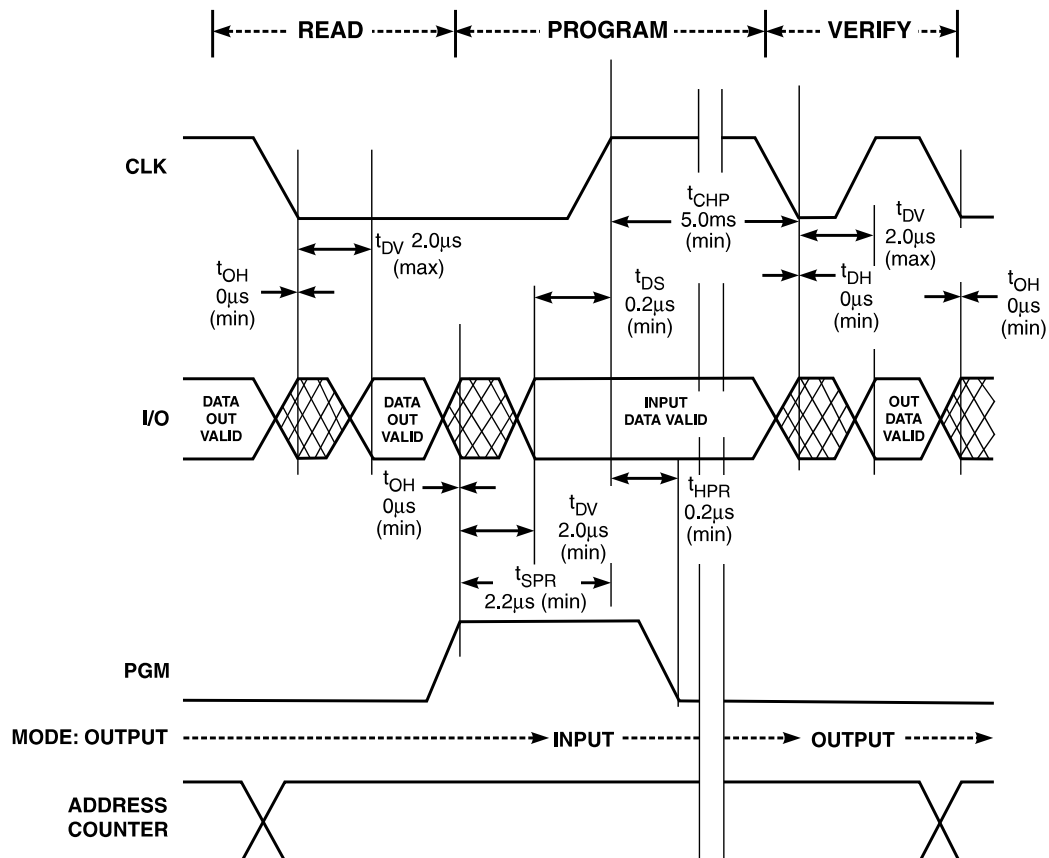
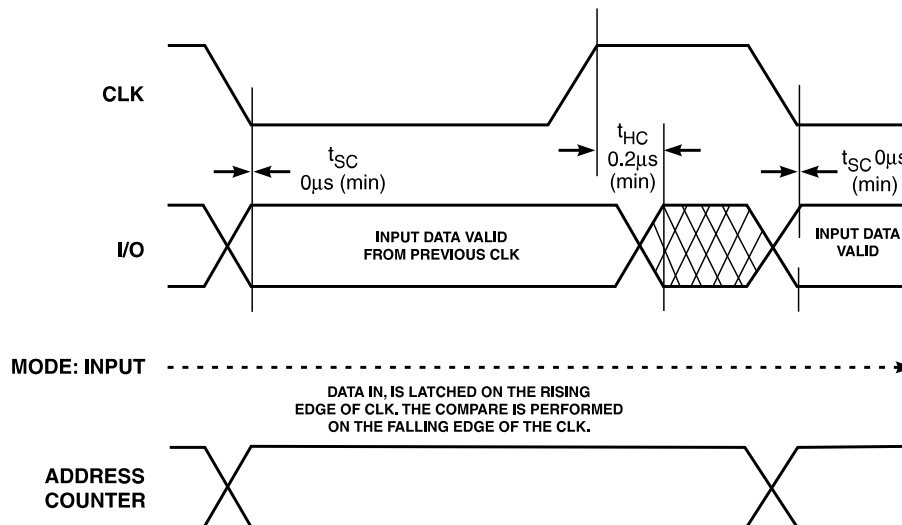


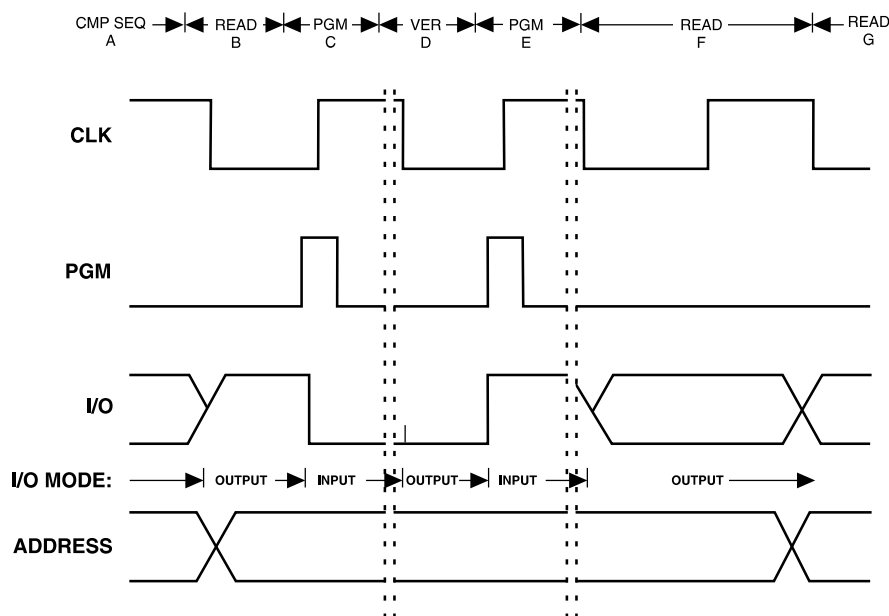
Figure 2. Read Timing







**Figure 5. SC and EZ1/EZ2 Validation for AT88SC101/102**



- A) Compare sequence of the security code or the application zone erase key.
- B) First bit which is at a logic 1, in the false attempts counter to validate SC, or in the recharge counter to validate EZ.
- C) Program sequence attempts to write a 0 over the 1 currently at this address.
- D) The chip outputs the new state of the bit. If a 0 has been successfully programmed, SC or EZ is set on the rising edge of PGM. (Note: If CLK rises when PGM is low, the validation is aborted.)
- E) This program sequence will erase either the false attempts counter or the application zone.
- F) Chip outputs state of the current bit. If the erase was successful, the chip will output a 1 if the current bit is in the false attempts counter. The chip will output a 0 if the current bit is in the recharge counter.
- G) On the falling edge of clock, the address is incremented and the state of the next bit is output.

Note: 1. The address does not change from operations B to F.



## Absolute Maximum Ratings\*

Operating Temperature..... -55°C to +125°C  
Storage Temperature..... -65°C to +150°C  
Voltage on Any Pin  
with Respect to Ground ..... -1.0 V to +7.0 V  
Maximum Operating Voltage ..... 6.6 V  
DC Output Current ..... 5.0 mA

\*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 is not implied. Exposure to absolute maximum rating conditions for extended periods may affect device reliability.

## DC Characteristics

Die  $T_{AMB} = -25^{\circ}\text{C}$  to  $70^{\circ}\text{C}$ ,  $V_{CC} = 5\text{V} \pm 10\%$ ,  $V_{SS} = 0\text{V}$  (unless otherwise specified)

Symbol	Characteristics	Min	Typ	Max	Unit
$I_{CC}$	Supply Current on $V_{CC}$ out of Program ( $t_{AMB} = +25^{\circ}\text{C}$ )	—	—	3.0	mA
$I_{CCP}$	Supply Current on $V_{CC}$ during Program ( $t_{AMB} = +25^{\circ}\text{C}$ )	—	—	4.0	mA
$V_{IL}$	Input Low Level	0	—	0.8	V
$V_{IH}$	Input High Level	2.0	—	$V_{CC}$	V
$V_{OL}$	Output Low Level ( $I_{OL} = 1\text{mA}$ )	—	—	0.4	V
$I_{Leak}$	I/O Leakage Current	-50	—	50	$\mu\text{A}$

Notes: 1. There is a pullup on pin RST.  
2. There are pulldowns on pins FUS, CLK and PGM.

## Packaging

All Atmel smart card secure ICs are available in wafer or standard packaging. Standard packages include plastic DIPs, SOICs, PLCCs.

## AC Characteristics

Die  $T_{AMB} = -25^{\circ}\text{C}$  to  $70^{\circ}\text{C}$ ,  $V_{CC} = 5\text{V} \pm 10\%$ ,  $V_{SS} = 0\text{V}$  (unless otherwise specified).

Symbol	Characteristics	Min	Typ	Max	Unit
$f_{CLK}$	Clock Frequency	—	—	300	KHz
$t_{CLK}$	Clock Cycle Time	3.3	—	—	$\mu\text{s}$
$t_{RH}$	RST Hold Time	20	—	—	$\mu\text{s}$
$t_{DVR}$	Data Valid Reset to Address 0	—	—	2.0	$\mu\text{s}$
$t_{CH}$	CLK Pulse Width (High)	0.2	—	—	$\mu\text{s}$
$t_{CL}$	CLK Pulse Width (Low)	0.2	—	—	$\mu\text{s}$
$t_{DV}$	Data Access	—	—	2.0	$\mu\text{s}$
$t_{OH}$	Data Hold	0	—	—	$\mu\text{s}$
$t_{SC}$	Data In Setup (CMP Instruction)	0	—	—	$\mu\text{s}$
$t_{HC}$	Data In Hold (CMP Instruction)	0.2	—	—	$\mu\text{s}$
$t_{CHP}$	CLK Pulse Width (High in Programming)	5.0	—	—	ms
$t_{DS}$	Data In Setup	0.2	—	—	$\mu\text{s}$
$t_{DH}$	Data In Hold	0	—	—	$\mu\text{s}$
$t_{SPR}$	PGM Setup	2.2	—	—	$\mu\text{s}$
$t_{HPR}$	PGM Hold	0.2	—	—	$\mu\text{s}$
$t_{DH}$	Data Hold from CLK	0	—	—	$\mu\text{s}$

## Conditions of Dynamic Tests

The circuit has an output with open drain. An external resistance is thus necessary between  $V_{CC}$  and I/O in order to load the output.

Pulse Levels of the Input:  $V_{SS}$  to 3.0V

Reference Levels in Output: 1.5V

Rising and Falling Time of Signals:  $< 5\text{ns}$

