Designing With CryptoAuthentication™ Client Devices

Overview

This document provides readers with an overview of the hardware circuitry recommended for deploying the CryptoAuthentication™ AT88SA102S chip in various configurations such as:

- **3 wire Configuration**
- **2 wire Configuration**
- **Host/Client Configuration or Multiple AT88SA102S chips sharing the same signal wire**
- **AT88SA102S with Super Capacitor**
- **USB CryptoAuthentication Dongle** (Rhino+)

This document also serves as a complete technical reference guide with key specifications, detailed schematics and the Bill of Materials needed for Rhino+ board.

CryptoAuthentication™ AT88SA102S Hardware Reference Design

Application Note

8667A–Crypto–5/09

1. Typical Setup

1.1. Three Wire Configuration

The AT88SA102S CryptoAuthentication chip is a cost-effective authentication chip designed to securely authenticate an item to which it is attached. It can also be used to facilitate exchange session keys with some remote entity so that the system microprocessor can securely encrypt/decrypt data. It is the first small authentication IC standard product to implement the SHA-256 hash algorithm, which is part of the latest set of recommended algorithms by the US Government. The 256 bit key space renders any exhaustive attacks impossible. The CryptoAuthentication family is available in a tiny 3-pin SOT23 package that provides a 1-wire communication interface (see Figure 1). The AT88SA102S pin descriptions can be found in Table 1.

Figure 1. AT88SA102S Standard 3-wire Configuration (V_{CC}, V_{SS}, and Signal)

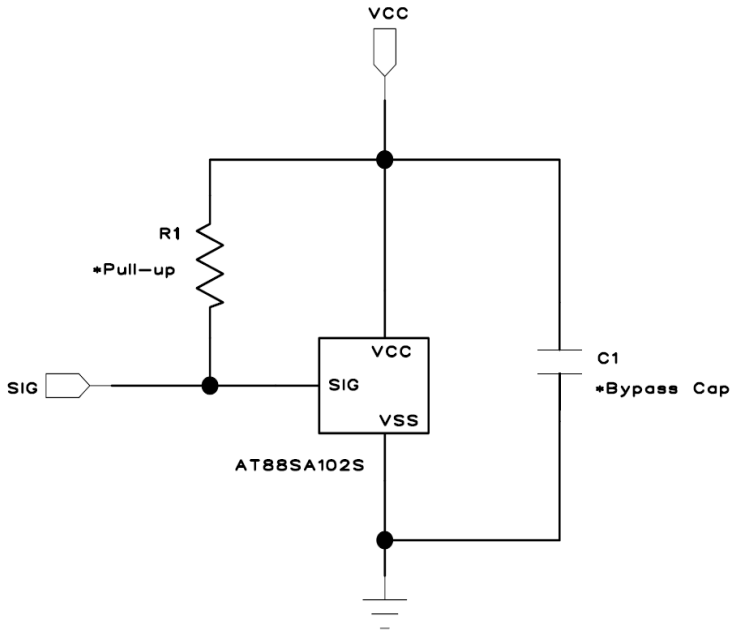


Table 1. AT88SA102S Pin Description

Pin #	Name	Description
1	Signal	IO channel to the system, open drain output. It is expected that an external pull-up resistor will be provided to pull this signal up to V_{CC} for proper communications. When the chip is not in use, this pin can be pulled to either V_{CC} or V_{SS}.
2	V_{CC}	Power supply, 2.5 – 5.5V. This pin should be bypassed with a high quality 0.01µF to 0.1µF capacitor close to this pin with a short trace to V_{SS}.
3	V_{SS}	Connect to system ground.

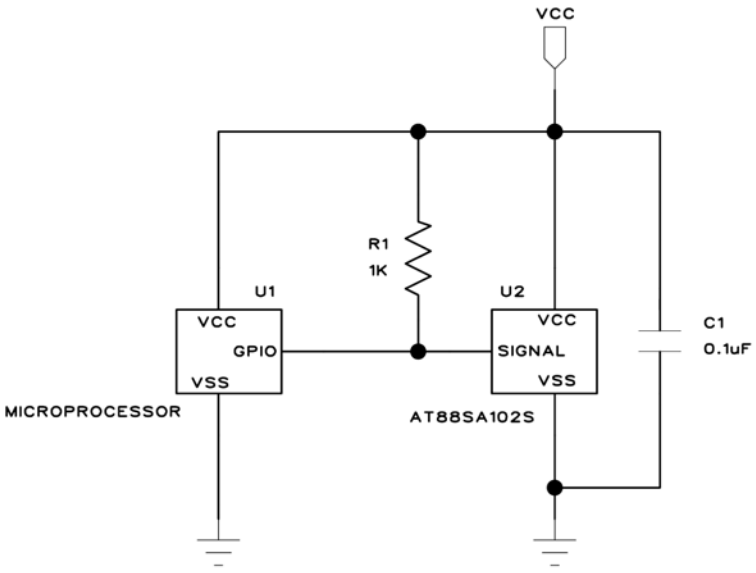
Note: See AT88SA102S datasheet for complete DC parameters.

2 Hardware Reference Design

1.1.1. Capacitor Selection

The role of the bypass capacitor, C1 in Figure 2, is to decouple the power supply bus from the IC. The act of decoupling eliminates the effects of the power bus inductance and resistance so that the transient currents flowing across the power bus do not cause excessive noise at the power and ground pins of the IC. Therefore, the bypass capacitor should have low effective series resistance (ESR) and series inductance while having a large enough capacitance value to supply current to the IC during switching. Careful observance of fundamental principles will determine how well the capacitor can suppress switching noise.

Figure 2. AT88SA102S Setup with Microprocessor



Typically, the value of the decoupling capacitor depends on the load the IC has to drive. Since the AT88SA102S is an open collector device, the load current (I_{Load}) refers to current requirements of the internal circuitry needed to pull the signal pin low.

$$I_{LOAD} = 1.0\ mA$$

The current demand is n*(I), where n is the number of outputs. Since the AT88SA102S only has one output, the demand is simply 1.0mA. The AT88SA102S has a V_{CC} tolerance on 5.0V (+0.5 /- 2.5V). If you consider some droop from the power bus, a switching time of 20nS, and allow a maximum voltage droop (ΔV) on the AT88SA102S of 0.025V (0.5%), the choice of bypass capacitor becomes

$$C = I_{Load}\frac{dt}{dv}$$

$$C = 800pF$$

With V_{CC} = 3.3V and a maximum allowable voltage droop of 0.015V (0.5%), C = 0.013uF. Choosing a value of 0.1µF will allow for variation due to temperature and aging for both V_{CC} conditions, 5V and 3.3V.

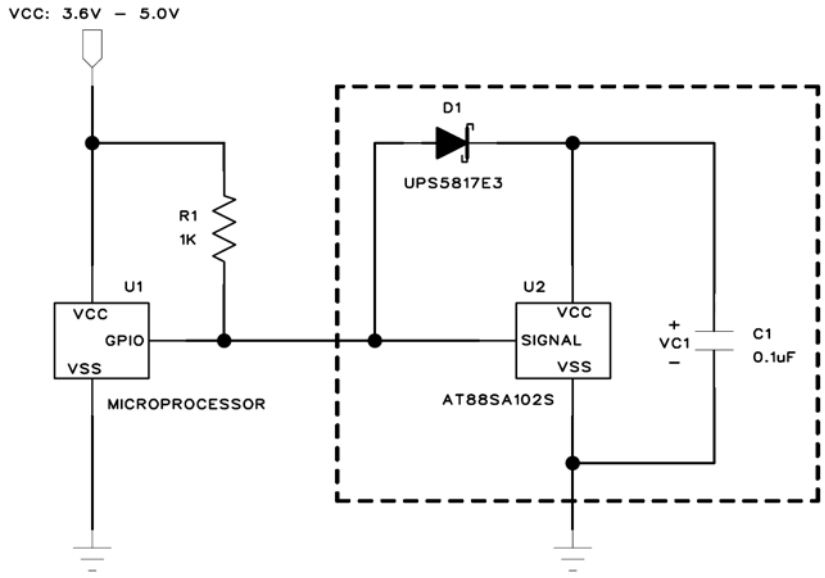
1.1.2. Placement

The placement of the capacitor in relationship to the IC is just as important as selecting the correct value. The decoupling capacitor should usually be placed as close as possible to the device requiring the decoupled signal. The goal is to minimize the amount of line inductance and series resistance between the decoupling capacitor and that device, and the longer the conductor between the capacitor and the device, the more inductance there is.

1.2. Two Wire Configuration

In Figure 3, the Schottky diode D1 connected between the Signal and V_{CC} pins permits the AT88SA102S to 'steal' power from the signal pin and store it on the bypass capacitor. This configuration permits the board containing the AT88SA102S and bypass capacitor C1 to be connected to the host microprocessor using just two wires, signal and ground.

Figure 3. AT88SA102S 2-wire Configuration



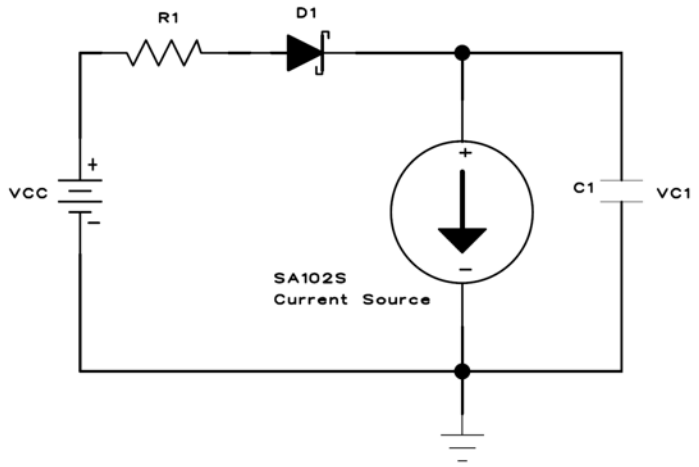
If a 1KΩ pullup resistor is used on the system side to pull the signal pin up to 3.6V (or higher), then the standard 0.1µF bypass capacitor is sufficient for proper operation. For lower supply voltages or higher resistor values the capacitor value will change.

1.2.1. Circuit Analysis, 2-Wire Configuration

Sections 1.2.1, 1.2.2, and 1.2.3 are given to provide insight into why the recommended values for R1 and C1 were chosen in Figure 3.

In Figure 3, the SIGNAL pin is pulled high by R1 during a t_{ZHI} pulse and while the AT88SA102S is sleeping. When the SIGNAL pin is high, current flows from V_{CC} through R1 and D1 to charge C1. The equivalent circuit when the SIGNAL pin is high is shown in Figure 4.

Figure 4. Equivalent Circuit when AT88SA102S SIGNAL is High.



Using Kirchhoff's Voltage Law on Figure 4, the final charge on C1, $V_{c1}(\infty)$, is given as:

$$V_{C1}(\infty) = V_{CC} - R1 \cdot I_{STATE} - V_{FD}$$

I_{STATE} = AT88SA102S supply current, state dependent

$V_{FD}(I_{STATE})$ = Diode Forward Voltage Drop, (Function of I_{STATE}) (1)

The AT88SA102S has different supply current requirements depending on the state. The different current requirements affect $V_{c1}(\infty)$. Given the following values:

$R1 = 1K$

$V_{CC} = 5.06V$

$I_{SLEEP} = 100nA$

$I_{STANDBY} = 60uA$

$I_{cc} = 550uA$

$V_{FD}(I_{SLEEP}) = 8mV$

$V_{FD}(I_{STANDBY}) = 190mV$

$V_{FD}(I_{cc}) = 190mV$

The final charges on $V_{c1}(\infty)$ are:

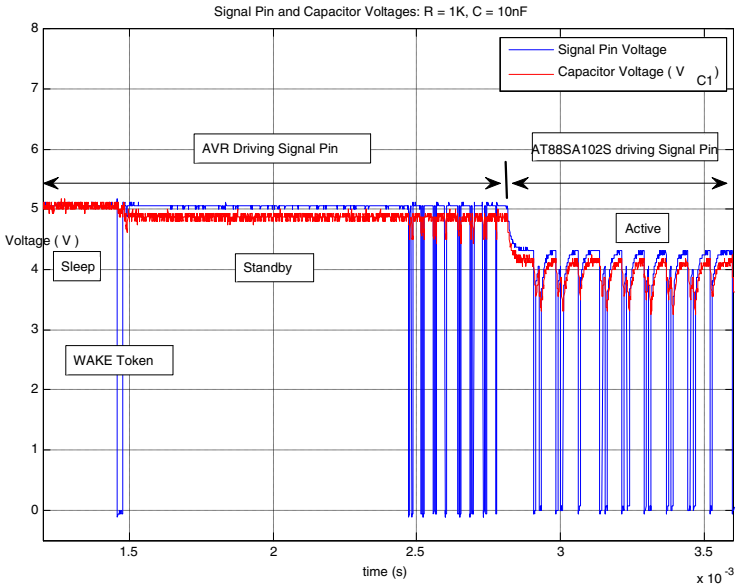
In sleep mode, $V_{C1}(\infty)_{SLEEP} = 5.05V$

In standby mode, $V_{C1}(\infty)_{STANDBY} = 4.81V$

In active mode, $V_{C1}(\infty)_{ACTIIVE} = 4.32V$

Figure 5 illustrates the different values of $V_{C1}(\infty)$ as a function of I_{STATE}.

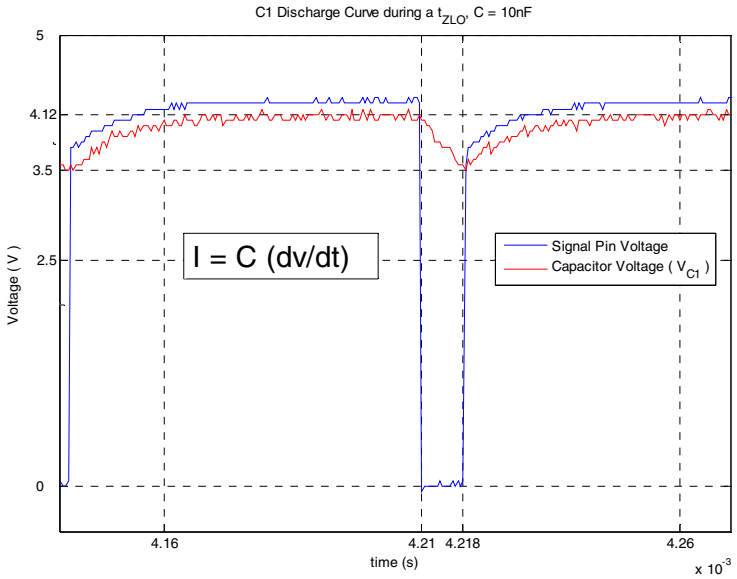
Figure 5. $V_{C1}(\infty)_{SLEEP,}$ $V_{C1}(\infty)_{STANDBY,}$ and $V_{C1}(\infty)_{ACTIVE}$.



1.2.2. Bypass Capacitor Selection

The AT88SA102S requires an additional 800uA to drive the SIGNAL pin low during a t_{ZLO} or a t_{START} pulse. This additional current load on C1 will cause it to discharge from $V_{C1}(\infty)_{active}$ according to dv = (C/I)dt (see Figure 6).

Figure 6. C1 Discharging during a t_{ZLO}



For the AT88SA102S to remain operational, V_{C1} must remain above the minimum supply voltage of 2.5V. Therefore, the value of C1 is chosen to ensure V_{C1} > 2.5V during a t_{ZLO} pulse. C1 is calculated using the following equations.

$$C1 = I_{ZLO}\frac{dv}{dt}$$

I_{ZLO} = 0.8mA, current requirements for t_{ZLO}

dt = 8.6µs, Max t_{ZLO} pulse

dv = $V_{C1}(\infty)_{active} - 3.3V$ = 1V

where $V_{C1}(\infty)_{active}$ = 4.3V

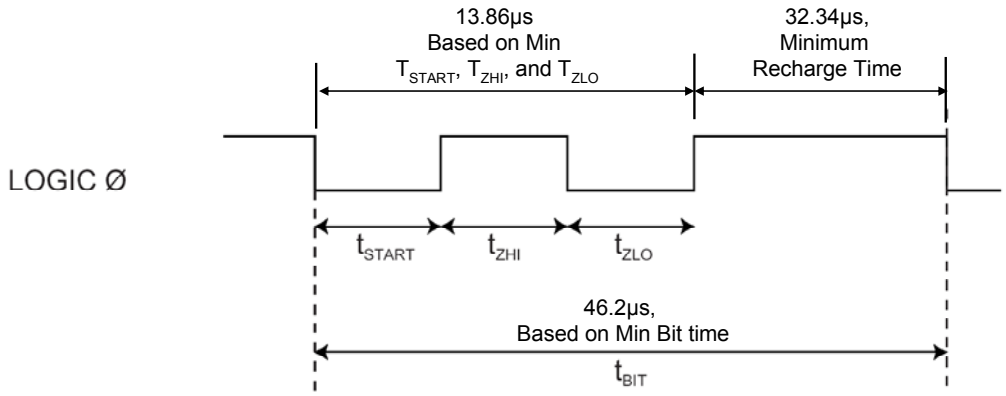
C1 = 6.9nF

Although 2.5V is the minimum supply voltage, 3.3V was chosen to allow for some margin. With C1 ≥ 6.9nF, V_{C1} will not drop below 3V during a maximum t_{ZLO} or a t_{START} pulse from the device.

1.2.3. Pullup Resistor Selection

The value of R1 in Figure 3 has two constraints. The first constraint requires that R1 allows sufficient current to flow to recharge C1 to $V_{C1}(\infty)_{active}$ in 32.34µs. The 32.34us is derived from the minimum Bit time of 46.2µs – Min (t_{START} + t_{ZHI} + t_{ZLO}), which is present with a LOGIC Ø device transmission (see Figure 7). Basically, C1 needs to recharge during the 32.34µs of t_{ZHI}'s to be ready for the next Bit transmission.

Figure 7. LOGIC Ø Waveform for minimum recharge time.



R1 second constraint requires the voltage on the SIGNAL pin ≤ V_{OL} (microprocessor) during a t_{ZLO} from the device. Using the following two equations (2) and (3), the boundary conditions for R1 are defined as:

The charge on V_{C1}: $$V_{C1}(t) = V_{C1}(\infty)_{active} + [V_{C1}(0) - V_{C1}(\infty)_{active}]e^{\left(\frac{-t}{R1C1}\right)} \quad (2)$$

This SIG pin voltage during a t_{ZLO}: $V_{CC} - R1*[\ I_{cmd} + i_{OL}\ (AT88SA102S)\ ]$ (3)

$$\frac{V_{CC} - V_{OL}(\text{microprocessor})}{I_{CC} + I_{OL}(\text{AT88SA102S})} \leq R1 \leq -\frac{t_{\text{worst case}}}{C1 \log\left[\frac{-0.02V_{C1}(\infty)\text{active}}{V_{C1}(t_{ZLO}) - V_{C1}(\infty)_{active}}\right]}$$

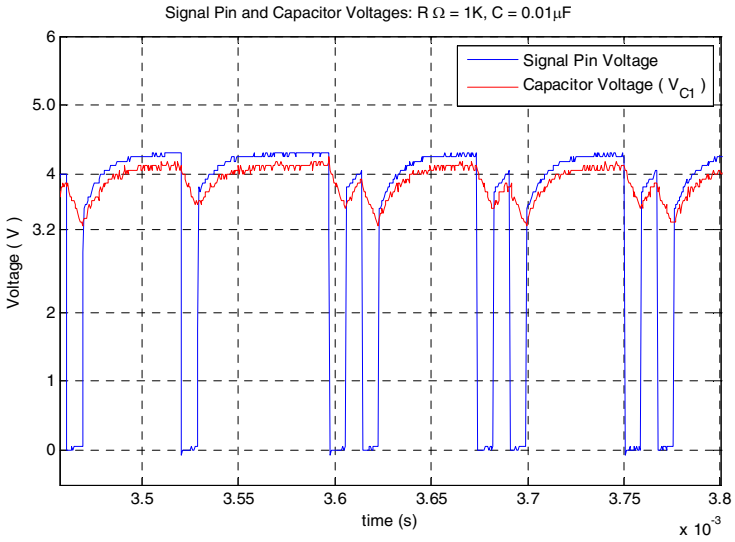
Since R1 is bounded as 900 Ω ≤ R1 ≤ 1.3K Ω, a 1KΩ resistor was chosen for this case study (see Figure 8).

The boundary conditions were calculated based on the following design specifications,

$$\begin{aligned} C1 &= 0.01\mu F \\ I_{OL}(\text{AT88SA102S}) &= 4mA \\ I_{cc} &= 550uA \\ V_{OL}\ (\text{microprocessor}) &= 1V \\ V_{C1}(\infty)_{\text{active}} &= 4.3V \\ V_{CC} &= 5.06V \\ t_{\text{worst case}} &= 32.3us \\ V_{C1}(t_{ZLO}) &= V_{C1}(\infty)_{\text{active}} - 1.4e\text{-}3*(dt/C) = 3.2 \end{aligned} \quad (4)$$

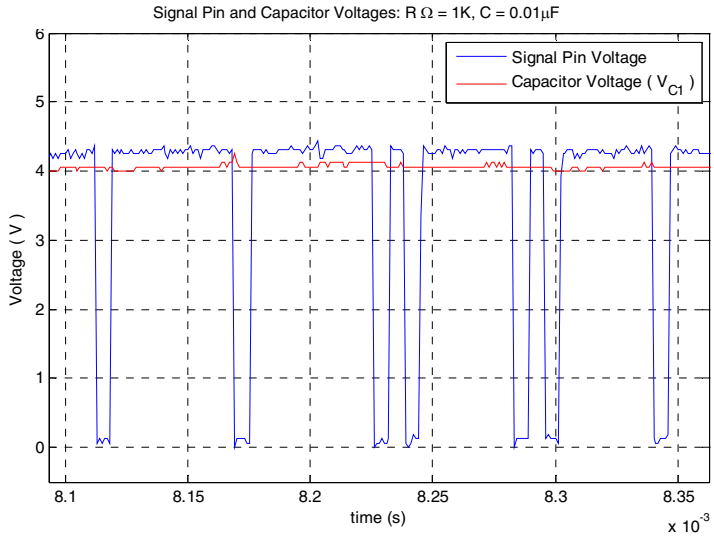
Equation (4) represents the voltage on C1 at the end of a t_{LZO} pulse for a LOGIC Ø device transmission. See Figure 8 at time step 3.7ms

Figure 8. $V_{C1}(t)$ Discharge and Recovery During a t_{ZLO} Pulse, C1 = 0.01μF



In Figure 8, we see that C1 = 0.01μF is sufficient to operate the AT88SA102S in the 2-wire configuration. However, increasing C1 = 0.1μF yields better performance in the sense of less droop on V_{C1} (see Figure 9).

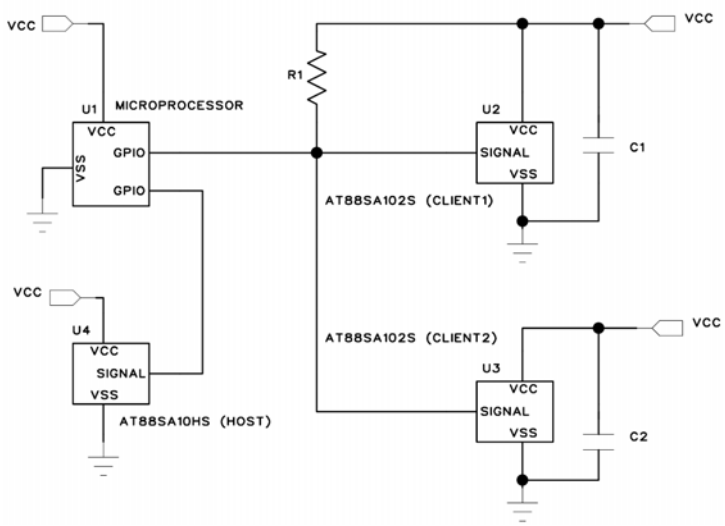
Figure 9. $V_{C1}(t)$ Discharge and Recovery During a t_{ZLO} Pulse, C1 = 0.1µF



1.3. Host / Client Configuration

Figure 10 shows the configuration used with the PauseLong command.

Figure 10. Multiple Authentication devices sharing same signal wire

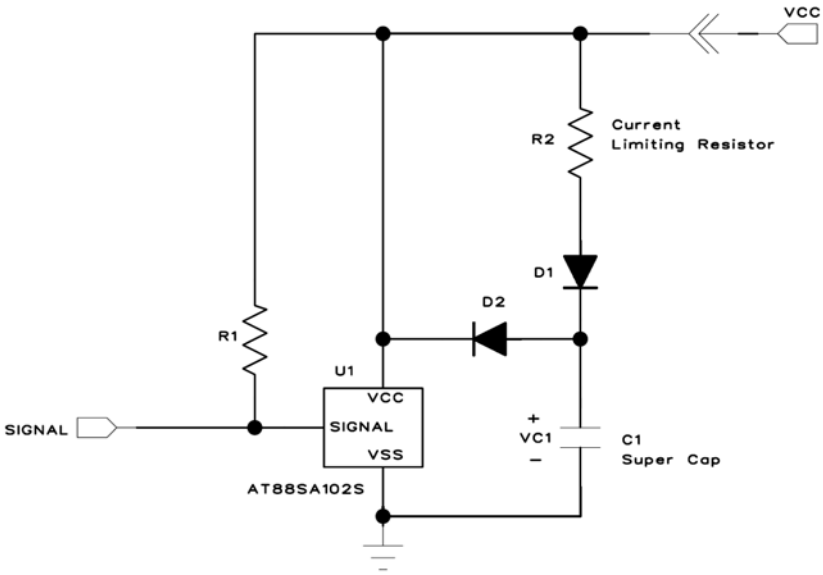


The PauseLong command forces the chip into a busy mode until the watchdog timer expires, after which it will automatically enter into the pause state. During execution of this command and while in the pause state the chip will ignore all activity on the IO signal. This command is used to prevent bus conflicts in a system that also includes other AT88SA102S chips or a CryptoAuthentication host chip sharing the same signal wire.

1.4. Super Capacitor Implementation

The super capacitor construction results in a low internal equivalent series resistance, making them ideal for delivering high peak current pulses without too much droop in the output voltage. Unfortunately, the low ESR presents a challenge during the charge cycle. When the supply voltage is first applied to an uncharged super capacitor, it looks like a low value resistor. This low ESR results in a large in-rush current if it is not controlled or limited. Failure to control the in-rush current may result in large voltage droop on the V_{CC} and possibly damage the power supply. Several possible solutions are available. One simple approach is to use a series resistor and two diodes (see Figure 11).

Figure 11. Super capacitor with a series resistor and 2 diodes setup



When V_{CC} is initially removed, the AT88SA102S effectively sees $V_{C1} = V_{CC} - 2V_{FD}$ (diode forward voltage drop). D2 prevents V_{CC} from bypassing the R2 and charging C1 directly. D1 prevents current flow through R1 once V_{CC} has been removed. Other than the in-rush current associated with super capacitor, they behave the same as other capacitors. Therefore, the capacitor requires a charge time of $t_{Charge} = 5*(R2*C1)$ for a full charge. Also, the discharge time of a capacitor with a constant discharge current can be calculated using the following equation.

$$t = C*(\Delta V / I) \quad (5)$$

Where,

t: Discharge time (sec.)

C: Capacitor capacitance (F)

ΔV: Working voltage range (V)

I: Discharge current (A)

As an example, the discharge time for the sleep state is:

$$V_{CC} = 5.0V$$

$$V_{FD} = 0.2V \text{ (Schottky, UPS5817E3)}$$

$$\Delta V = (V_{CC} - 2V_{FD}) - 2.5V = 2.1V$$

$$t = 330mF*(1.3 /100nA) = 80.2 \text{ days}$$

$$\text{With } V_{CC} = 3.3V,\ t = 330mF*(1.3 /100nA) = 7.6 \text{ days}$$

The actual discharge time will vary if the AT88SA102S transitions between states. The above equation only accounts for a constant discharge current within a particular state. For instance, the AT88SA102S current consumption is different for I_{SLEEP} vs. I_{cc}. To account for the transitions between these states, equation (5) was modified to include I_{cc} duty cycle.

$$t = \frac{C \cdot \Delta V}{(I_{SLEEP} + I_{CC} \cdot \text{duty cycle})}$$

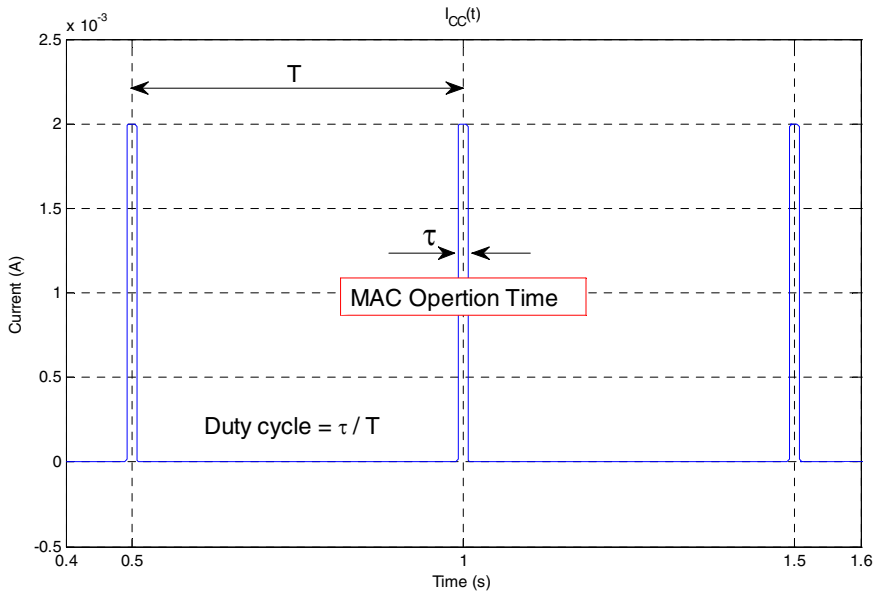
For example, given that

$$I_{CC} = 2mA$$

$$I_{SLEEP} = 100nA$$

AT88SA102S performs a MAC every 500ms (T) with an operation time of 15ms (τ) (see Figure 12).

Figure 12. AT88SA102S Supply Current $I_{cc}(t)$ Duty Cycle



The discharge times are

$$t = \frac{0.33F \cdot 2.1V}{(100nA + 2mA * (3ms/500ms))} = 15.9Hrs$$, for V_{CC} = 5.0V

$t = 9.8Hrs$, for V_{CC} = 3.3V

The sleep command should be used to force the AT88SA102S device into the low power state to conserve power. As a fail-safe, the CryptoAuthentication Watchdog Failsafe timer will force the AT88SA102S into sleep mode after $t_{WATCHDOG}$ has elapsed.

2. Rhino+ Hardware Description

2.1. Rhino+ Overview

This section describes the Rhino+ board (see Figure 13) which is designed to allow an easy evaluation of the AT88SA102S CryptoAuthentication chip. This low-cost compact USB dongle design combines the ATMEL ATtiny85 microcontroller and the AT88SA102S-TSX-T CryptoAuthentication chip. The USB interface is suitable for applications such as:

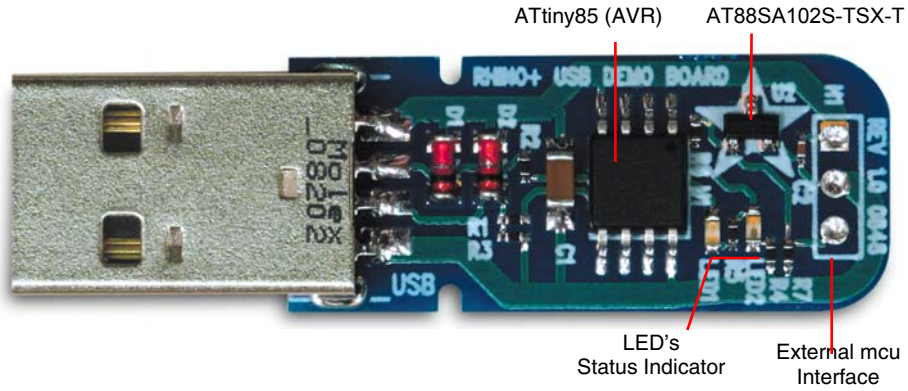
- USB security dongles
- Encrypted downloads
- Media transmission encryption
- See Application Note: 929-8563A CryptoAuthentication Product Uses

Rhino+ provides the following features:

- ATtiny85, Low Power AVR® 8-Bit Microcontroller , 8K Byte Flash Memory
- AT88SA102S CryptoAuthentication Chip
- USB Interface to PC
- 1 3-pin header to interface AT88SA102S with an external microcontroller
- 2 Status LED status indicator

For application software, application notes and datasheet please visit www.atmel.com/rhino.

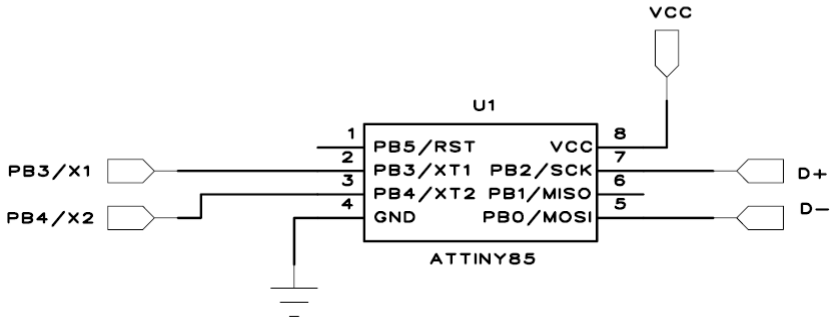
Figure 13. Rhino+ CryptoAuthentication USB Dongle



2.2. Microcontroller

The ATtiny85 microcontroller handles the USB communication between the PC and AT88SA102S device (see Figure 14). The USB protocols are implemented on the AVR using a firmware stack that is USB 1.1 compliance. The AVR also contains the drivers that handle the AT88SA102S 1-wire protocols. The USB firmware stack and the AT88SA102S drivers consume less than 6K Byte of memory.

Figure 14. ATtiny85 AVR Microcontroller USB Configuration

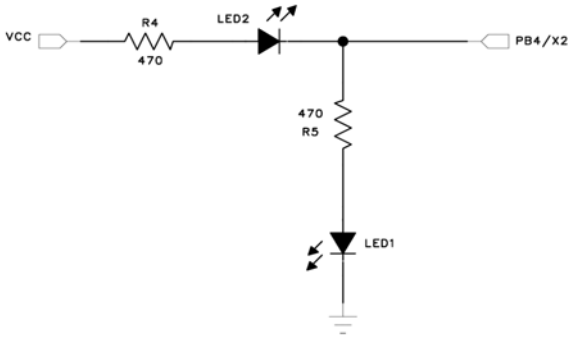


See the ATtiny85 datasheet for detailed information, www.atmel.com

2.3. Description of User LEDs

Rhino+ has 2 LEDs which are connected to PB4 (AVR) (see Figure 15). They can be used as status indicators.

Figure 15. Implementation of User LEDs



Tri-stating PB4 will turn on both LEDs; otherwise, the LEDs will toggle. This configuration also serves as a power indicator since at least 1 LED is always on. The AVR can source or sink enough current to drive a LED directly.

2.4. Description of 3-Pin Header

Header H1 enables the user to interface directly with the AT88SA102S chip with an external microcontroller (see Figures 16 and 17). At power-up, PB3 (onboard AVR) is tri-stated and therefore will not infer with the external microcontroller driving the SIG line. Although not necessary, R8 can be removed to totally eliminate any possibility of contention between the PB3 /X1 and an external microcontroller driving the SIG line simultaneously.

Figure 16. External Interface Header on Rhino+

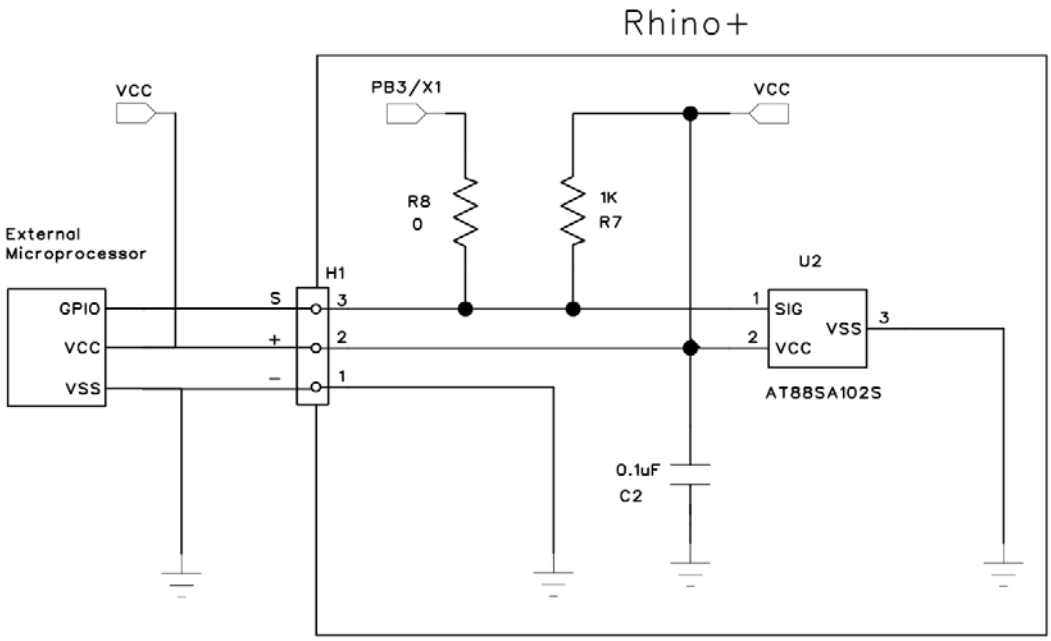
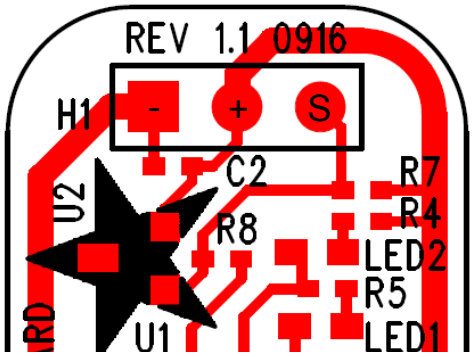


Figure 17. PCB Layout of the External Interface Header Signals for Rhino+



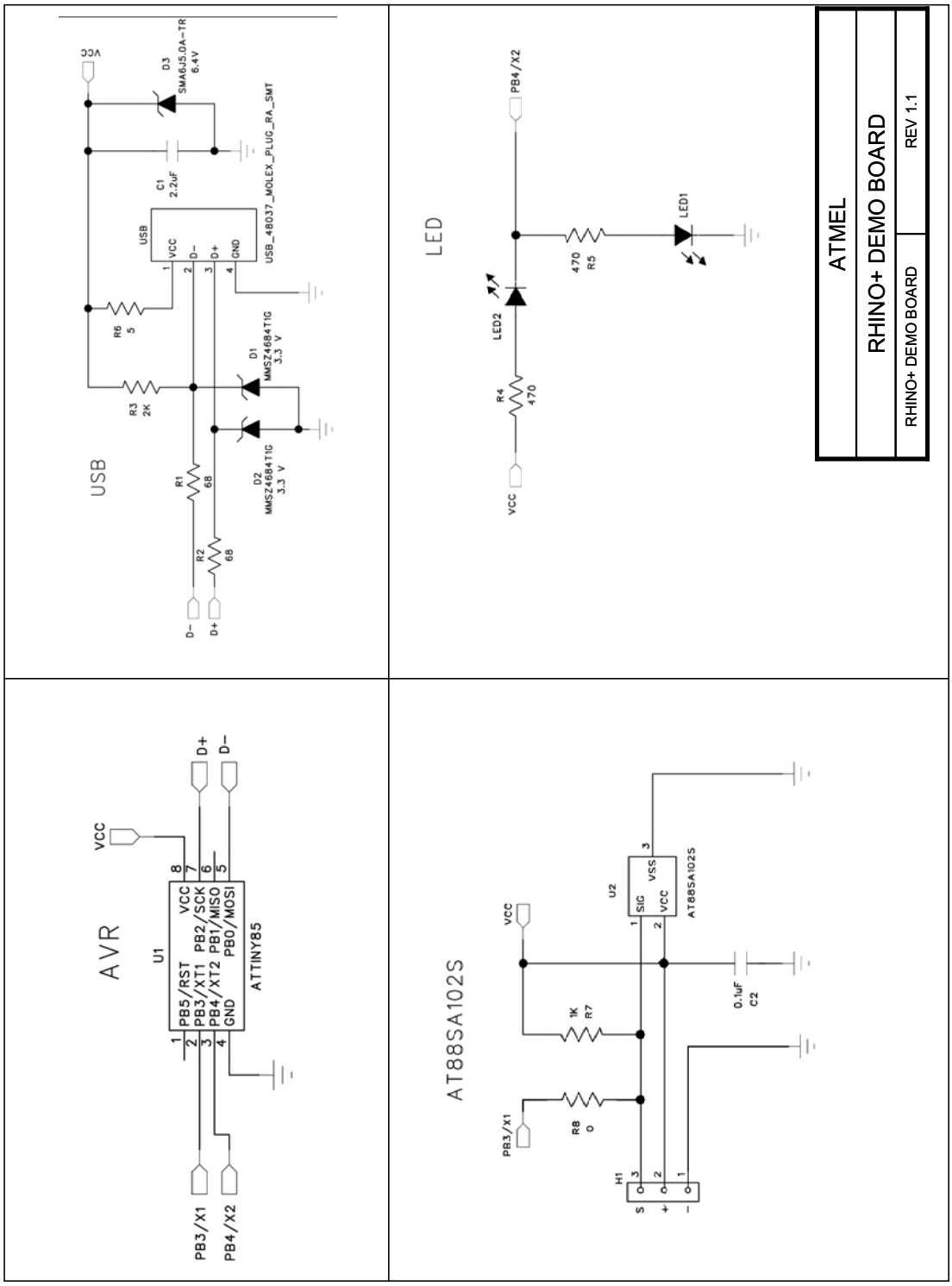
2.5. Rhino+ Bill of Materials

Table 2. Rhino+ Bill of Materials

Designator	Value	Description	Manufacture Part #	Footprint	Quantity
R1, R2	68 +/- 5%	Resistor	ERJ-2GEJ680X	0402	2
R3	2.2K +/- 5%	Resistor	ERJ2GEJ222X	0402	1
R4, R5	470 +/- 5%	Resistor	ERJ2GEJ471X	0402	2
R6	4.87 +/- 1%	Resistor	CRCW06034R87FNEA	0805	1
R7	1K +/- 5%	Resistor	ERJ2GEJ102X	0402	1
R8	0 Ω	Resistor	CR0402-16W-000T	0402	1
C1	2.2µF +/- 10%	Capacitor	ECJ-2FB1C225K	0805	1
C2	0.1µF +/- 10%	Capacitor	C0402X7R160-104KNE	0402	1
D1, D2	3.6V	Zener Diode	ZMM5227B-7	Mini MELF	2
D3	6.5V	TVS Diode (Optional)	SMA6J5.0A-TR	DO-214AC, SMA	1
LED1	Red	SMD	BR1111C-TR	0603	1
LED2	Blue	SMD	MB1111C-TR	0603	1
U1	ATtiny85	AVR	ATMEL	SOIC-8ld	1
U2	AT88SA102S	Crypto-Authentication	ATMEL	3 Pin SOT-23	1
USB	USB, Right Angle	Type A connector	48037-1000	SMT	1

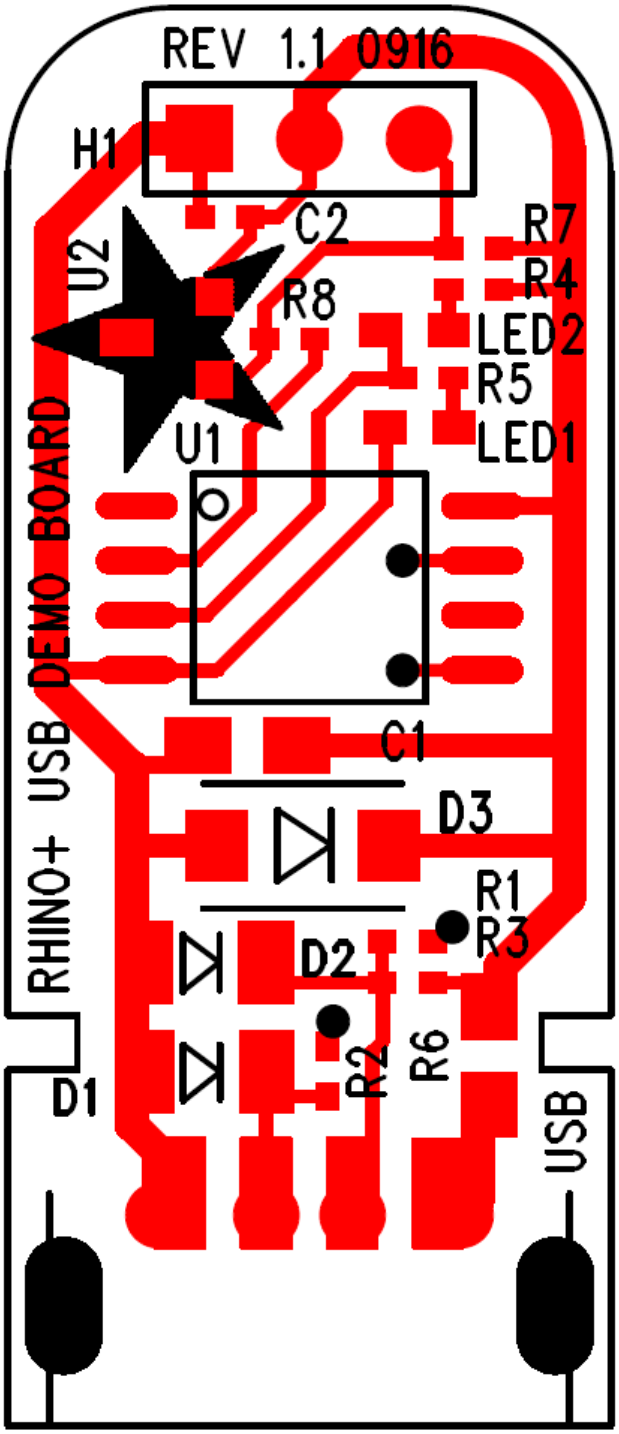
2.6. Rhino+ Complete Schematic

Figure 18. Complete Schematic for Rhino+



2.7. Rhino+ PCB Layout

Figure 19. Top Layer PCB Layout for Rhino+, Single-Sided PCB



Appendix A. Revision History

Doc. Rev.	Date	Comments
8667A	05/2009	Initial document release

Headquarters

Atmel Corporation
2325 Orchard Parkway
San Jose, CA 95131
USA
Tel: 1(408) 441-0311
Fax: 1(408) 487-2600

International

Atmel Asia
Room 1219
Chinachem Golden Plaza
77 Mody Road Tsimshatsui
East Kowloon
Hong Kong
Tel: (852) 2721-9778
Fax: (852) 2722-1369

Atmel Europe
Le Krebs
8, Rue Jean-Pierre Timbaud
BP 309
78054 Saint-Quentin-en-
Yvelines Cedex
France
Tel: (33) 1-30-60-70-00
Fax: (33) 1-30-60-71-11

Atmel Japan
9F, Tonetsu Shinkawa Bldg.
1-24-8 Shinkawa
Chuo-ku, Tokyo 104-0033
Japan
Tel: (81) 3-3523-3551
Fax: (81) 3-3523-7581

Product Contact

Web Site
www.atmel.com

Technical Support
pcsecurity@atmel.com

Sales Contact
www.atmel.com/contacts

Literature Requests
www.atmel.com/literature

8667A–Crypto–5/09