APPLICATION NOTE

Migrating AT88SA102S to ATSHA204

Features

- Configuration of the Atmel® ATSHA204 for hardware compatibility with the Atmel AT88SA102S
- The ATSHA204 authentication compatiblility with the AT88SA102S
- The ATSHA204 Read compatiblility with the AT88SA102S Fuse Read

Description

This application note describes how to configure the ATSHA204 so the device can act as an AT88SA102S replacement.

As members of the Atmel CryptoAuthentication™ family, the AT88SA102S and the ATSHA204 devices use the SHA-256 algorithm for system authentication, key storage/exchange, and other related uses. While the ATSHA204 offers a wide array of features and EEPROM storage, it was designed to be backwards compatible to the AT88SA102S. Most application systems designed to use the AT88SA102S can be easily upgraded to use the ATSHA204 without requiring any hardware or software changes in the Host or Client.

The package is identical for all devices as is the I/O protocol; so no board changes are required nor are any changes required for the low level I/O drivers.

1. ATSHA204 Authentication Compatibility

The ATSHA204 is designed to be backwards compatible to the AT88SA102S for field operation. Most systems designed to use the AT88SA102S in Client devices will work perfectly with the ATSHA204 in the Client devices without any modification to the Host system software or hardware.

When using the AT88SA102S for authentication, a MAC command is executed and the response is compared to an identical calculation on the Host. The ATSHA204 device can be configured such that its MAC command will match the AT88SA102S MAC response for all modes.

1.1 ATSHA204 Configuration

For compatibility with the AT88SA102S, the following values should be written to the memory of the ATSHA204:

1. During configuration, OTPmode should be set to Legacy to hide the values of the first 64 bits of the OTP section, which contain a secret in the AT88SA102S.
2. The same secret and status information that would have been written to the first 88 fuse bits of the AT88SA102S should be written to the first 88 bits of the OTP section on the ATSHA204.
3. OTP bits 88 through 95 should be written with the value stored in SN[8] within the Configuration zone of the ATSHA204 device. The Read command on legacy systems will always use the values in the OTP zone, while the ATSHA204 always uses the values in the Configuration zone during the computation of cryptographic results.
4. OTP bits 96 through 127 should be written with copies of the values stored in SN[4:7] within the Configuration zone of the ATSHA204 device.
5. The key slot identified by the least significant four bits of the AT88SA102S SlotID assigned to a particular customer should be loaded with the Atmel provided value for that key.
6. The SlotConfig bits for the key slot identified in Step 5 should be set to: CheckOnly=0, SingleUse=0, EncryptRead=0, IsSecret=1, WriteConfig=1000.

1.1.2 OTP Mode Set to *Legacy*

The OTP mode setting in the Configuration zone should be set to Legacy mode (0x00).

0x00 (Legacy mode) = When OTP zone is locked, writes are disabled, reads to Word 0 and Word 1, and 32-byte reads are disabled.

1.1.3 OTP Zone Byte Map

The issues to consider when configuring the OTP zone on the ATSHA204 are to duplicate the existing MAC *and the* Fuse Read commands for the AT88SA102S. The Fuse Read command for the AT88SA102S uses mode = 01. This corresponds to an OTP Zone Read on the ATSHA204.

The OTP zone of the ATSHA204 should be configured as follows:

Figure 1-1. ATSHA204 OTP Zone Configuration

Byte Count	OTP Bytes	Fuses (Bits)	Description
8	0x00 – 0x07	0 – 63	AT88SA102S Secret Fuses + BurnFuse Enable bit
3	0x08 – 0x0A	64 – 83	23 Status Fuses + Fuse Disable Bit.
1	0x0B	88 – 95	AT88SA102S: Fuse MfrID (8-bits). ATSHA204: SN[8]. Copied from the Configuration Zone.[1]
4	0x0C-0x0F	96 – 127	AT88SA102S: Fuse SN (32-bits) ATSHA204: SN[4:7]. Copied from the Configuration Zone. [1]

Note: 1. Each device's SN bytes need to be copied from the Configuration Zone to the designated location in the OTP Zone. This ensures that the AT88SA102S Read commands will behave identically.

1.1.4 Key Value Configuration

The values stored in the AT88SA102S internal key array are hardwired into the masking layers of the device during wafer manufacture. Individual key ID and corresponding key values are made available to qualified customers upon request to Atmel.

The ATSHA204 does *not* have internal key values; therefore, the AT88SA102S internal key value must be explicitly programmed into a key-specific slot on the ATSHA204.

Follow these steps to configure the AT88SA102S internal keys to ATSHA204:

1. Mask the AT88SA102S key ID to determine the slot. (See examples below)
2. Wrtie the key value obtained from Atmel to the slot indicated in Step 1.

The MAC command of the ATSHA204 will mask all but the least significant four bits of the KeyID (Param2). Param2 will appear on the bus least-significant byte first. Below are some examples.

Figure 1-2. Examples

AT88SA102S Key ID	Param 2 (On the Bus)	ATSHA204 Slot
5492	9254	2
7D8E	8E7D	E

1.2 ATSHA204 Authentication Calculation

Once the ATSHA204 is configured properly, the result of its MAC command will match the AT88SA102S MAC command for all modes. The message sent to the SHA-256 calculation is illustrated in the following table.

Table 1-1. Message Bytes for SHA-256 Calculation

Byte Count	AT88SA102S	ATSHA204	Example Bytes	Notes
32 (256-bits)	key[KeyID]	key[KeyID]	`00 01…1E 1F`	AT88SA102S: Internal key from Atmel. ATSHA204: Slot has the same value as the AT88SA102S internal key.
32 (256-bits)	Challenge	Challenge	`10 11…2E 2F`	System can send any bytes for challenge.
1 (8-bits)	Opcode	Opcode	`08`	MAC opcode is the same for both devices.
1 (8-bits)	Mode	Mode	`50`	Bit 4: Include 88 OTP bits (OTP[0:10]) in the message. Bit 6: Include 48 SN bits (SN[2:3] & SN[4:7]) in the message.
2 (16-bits)	KeyID	Param 2	`92 E3`	Least significant byte first on the bus. Note: The full KeyID should be sent to the ATSHA204.
8 (64-bits)	Secret Fuses	OTP[0:7]	`20 21…26 27`	Programmable Secret
3 (24-bits)	Status Fuses	OTP[8:10]	`89 AB CD`	Programmable Fuses (bytes)
1 (8-bits)	Fuse MfrID	SN[8]	`EE`	Never zero'd out.
4 (32-bits)	Fuse SN	SN[4:7]	`01 FC BF 7F`	Bytes will be zeros depending on mode.
2 (16-bits)	ROM MfrId	SN[0:1]	`01 23`	Never zero'd out.
2 (16-bits)	ROM SN	SN[2:3]	`50 7B`	Bytes will be zeros depending on mode.

2. Revision History

Doc. Rev.	Date	Comments
8864A	03/2013	Initial document release.

Enabling Unlimited Possibilities®

Atmel Corporation 1600 Technology Drive, San Jose, CA 95110 USA **T:** (+1)(408) 441.0311 **F:** (+1)(408) 436.4200 | **www.atmel.com**

Disclaimer: The information in this document is provided in connection with Atmel products. No license, express or implied, by estoppel or otherwise, to any intellectual property right is granted by this document or in connection with the sale of Atmel products. EXCEPT AS SET FORTH IN THE ATMEL TERMS AND CONDITIONS OF SALES LOCATED ON THE ATMEL WEBSITE, ATMEL ASSUMES NO LIABILITY WHATSOEVER AND DISCLAIMS ANY EXPRESS, IMPLIED OR STATUTORY WARRANTY RELATING TO ITS PRODUCTS INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NON-INFRINGEMENT. IN NO EVENT SHALL ATMEL BE LIABLE FOR ANY DIRECT, INDIRECT, CONSEQUENTIAL, PUNITIVE, SPECIAL OR INCIDENTAL DAMAGES (INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS AND PROFITS, BUSINESS INTERRUPTION, OR LOSS OF INFORMATION) ARISING OUT OF THE USE OR INABILITY TO USE THIS DOCUMENT, EVEN IF ATMEL HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. Atmel makes no representations or warranties with respect to the accuracy or completeness of the contents of this document and reserves the right to make changes to specifications and products descriptions at any time without notice. Atmel does not make any commitment to update the information contained herein. Unless specifically provided otherwise, Atmel products are not suitable for, and shall not be used in, automotive applications. Atmel products are not intended, authorized, or warranted for use as components in applications intended to support or sustain life.