APPLICATION NOTE

Personalization Guide

Atmel ATSHA204

Introduction

Before using the Atmel® ATSHA204 device, there are some initialization processes that need to be performed first. The initialization processes consist of personalizing the device and then lock the device.

In the personalization step, the device behavior, the data slot behavior, and the data itself is being configured as desired. After the personalization process is performed, the device needs to be locked to prevent any further modification to data. Details of the initialization processes are described within this document.

Overview

The initialization process consists of four basic steps:

- **Personalize Configuration Zone —** Personalize device configuration such as I2C_Address, OTPMode, SelectorMode, SlotConfig, UseFlag, LastKeyUse, and Selector Value.
- **Lock Configuration Zone —** Lock Configuration zone after the Configuration zone has been personalized. Atmel recommends including CRC checksum in the lock process to ensure that the device has been personalized as desired.

  Configuration zone must be locked to enable the personalization of Data/OTP zones. Prior to locking Configuration zone, Data/OTP zone cannot be read nor written at all.
- **Personalize Data/OTP Zones —** Personalize Data zone to store data such as keys, calibration data, model number, etc.

  Personalize OTP zone to store fixed data such as model numbers, calibration information, manufacturing history, or other data that should never change.
- **Lock Data/OTP Zones —** Lock Data/OTP zones after writing Data and OTP zones. Atmel recommends including CRC checksum in the lock process to ensure the data written are as desired.

1. Personalize Configuration Zone

There are some bytes that should be configured before using the ATSHA204 device. These bytes are used to control the access permission information for each slot of the data memory and to personalize the device behavior itself.

The details of these bytes are described below. For more information, please refer to latest ATSHA204 datasheet.

- **I2C_Address —** I2C_Address is represented by byte 16 of the Configuration zone. It holds 0xC8 as default value. This byte is mainly used to identify the device in I^2C communication. This byte can also be used to control the input level for the ATSHA204.
- **OTPMode —** This OTPMode is represented by byte 17 of the Configuration zone. It holds 0x55 as default value. This byte is used to control the permission level of OTP zones. OTP zone can be used as additional message body for generating MAC, HMAC, or Gendig response, according to the command mode.
- **SelectorMode —** This byte is used to control the write permission to Selector byte. This SelectorMode is represented by byte 19 of the Configuration zone. It holds 0x00 as default value. If this byte is set to 0x00, the Selector byte can always be modified with UpdateExtra command. If this byte is set to a non-zero value, the Selector byte can only be written if it currently has a value of zero.
- **Slot Configuration —** Slot Configuration bytes are represented by byte 20 – 51. Each slot uses two bytes to determine the slot behavior, byte 20 and byte 21 are the configuration bytes for key slot 1, byte 22 and byte 23 which are the configuration bytes for key slot 2, and so on.

  Note: The even bytes are LSBytes —– it holds bits 0:7, while the odd bytes are MSBytes — it holds bits 8:15. For example, slot 1 configuration bytes are byte 20 and byte 21, bits 0:7 are hold by byte 20, while bits 8:15 are hold by byte 21.

  See Table 1-1 for details of the 2-byte configurations of each slot.

Table 1-1. 2-byte Slot Configurations

SlotConfig	Comments
ReadKey	ReadKey is used to determine which KeyID will be used to generate the encryption key to encrypt the data being read from the corresponding slot. ReadKey is represented by bits 3:0 of the slot configuration.
CheckOnly	CheckOnly is used to determine that the corresponding slot is used for CheckMac command only or can be used for another crypto command. CheckOnly is represented by bit 4 of the slot configuration.
SingleUse	SingleUse is used to determine whether the usage of the corresponding slot is limited or not. SingleUse is represented by bit 5 of the slot configuration. This limitation only applied to slot 0 – 7.
EncryptRead	EncryptRead is used to determine that reading from the corresponding slot must be encrypted or not. EncryptRead is represented by bit 6 of the slot configuration.
IsSecret	IsSecret is used to determine that the corresponding slot is secret or not. IsSecret is represented by bit 7 of the slot configuration.
WriteKey	WriteKey is used to determine which KeyID will be used to validate and encrypt data written to the corresponding slot. WriteKey is represented by bits 11:8 of the slot configuration.
WriteConfig	WriteConfig is used to determine the modification ability of the corresponding slot. WriteConfig is represented by bits 15:12 of the slot configuration. There are two ways to modify the data in the slot; by using Write command and by using DeriveKey command. The WriteConfig control the ability of these two commands to modify the data.

- **UseFlag —** UseFlag is represented by even byte from byte 52 to 66. Byte 52 corresponds to Key0, 54 to Key1, and so on.

  These bytes are used to indicate how many times a key may be used. This limitation is only applied to key slot 0 – 7.

  By default, this byte is set to 0xFF. Each time the key is used, a UseFlag bit changed from one to zero and it starts from the most significant bit to the least significant bit. By default, a key may be used eight times before it must be refreshed by using a Write command or DeriveKey command; however, these limitations can be reduced by clearing some of the most significant bit, into 0x7F (seven uses), 0x3F (six uses), 0x1F (five uses), and so on.

  Atmel recommends that the key to be used a single time only, with the other chance of uses providing a safety margin for errors.
- **LastKeyUse —** LastKeyUse is represented by bytes 68 – 83. The default value of these bytes is 0xFF. These bytes act similarly like UseFlag, but they are only applied to Key15. Each time Key15 is used, the same mechanism as UseFlag is applied here. Therefore, this key can be limited up to 128 uses. The user can reduce the use limitation by setting these bytes the exact same way as setting the UseFlag byte. The total number of bits set to one indicates the number of usage limitations.

  After all the LastKeyUse reached 0x00, key15 is permanently disabled. There is no mechanism reset the LastKeyUse bytes.
- **Selector —** Selector is represented by byte 85. The default value of this byte is 0x00. This byte is used to select which chip will remain in active mode after the execution of pause command. This byte cannot be modified by using normal write command; instead it can only be updated using UpdateExtra command.

2. Lock Configuration Zone

After the ATSHA204 device is configured, the next step is to lock Configuration zone. Prior to locking Configuration zone, neither read nor write is permitted to the Data/OTP zones; therefore, the Configuration zone must be locked before personalizing Data and OTP zones.

Atmel recommends using CRC checksum in the lock process to ensure the device has been configured as desired. ATSHA204 uses CRC-16 algorithm to generate a summary digest of the designated zones. For Configuration zone, the CRC is calculated over all 88 bytes of the Configuration zone. If the CRC does not match, an error is returned from the device, indicating there is data mismatch. If there is data mismatch, the personalization process needs to be repeated to ensure every personalization is as desired.

3. Personalize Data/OTP Zones

Data zone consists of 512 bytes split into 16 general-purpose, read-only, or read/write memory slots; each consisting of 32 bytes. Each slot can be used to store keys, calibration data, model number, or other information related to the item to which the ATSHA204 device is attached. Not all slots can be written because it depends on the slot configuration. It cannot be written at all if the slot write-configuration is set to Never. If the write-configuration is set to Encrypt, then only encrypt write is permitted to write to the corresponding slot.

OTP zone consists of 64 bytes of one-time programmable (OTP) bits. The OTP zones can be used to store fixed data such as, model numbers, calibration information, manufacturing history, or other data that should never change. These bytes can freely be written after the Configuration zone has been locked, but prior to Data/OTP zones locked.

4. Lock Data/OTP Zones

Upon completion of any writes, the data and OTP sections should be locked. It is important that the data and OTP sections be locked prior to release of the system containing the device into the field. Failure to lock these zones may permit modification of any secret keys and may lead to other security problems.

Atmel recommends using CRC checksum in the lock process to ensure the data written are as desired. ATSHA204 uses CRC-16 algorithm to generate a summary digest of the designated zones. For the Data and OTP zones locked, the contents are concatenated in the order to create the input to the CRC algorithm. If the CRC does not match, an error is returned from the device, indicated that there is data mismatch; therefore the personalization process needs to be repeated.

5. Personalization Example

This section gives an example of the desired device personalization and the corresponding bits setting for the device.

5.1 Accessory Authentication Use Case

Two ATSHA204 devices are used in an accessory authentication, such as battery authentication. In this case, ATSHA204 is embedded in a mobile device as Host and in the battery as Client. The diversified key scheme is also utilized in this example case. The communication protocol used between MCU and ATSHA204 is I^2C protocol.

5.1.1 Host ATSHA204 Personalization

The personalization of the Host for this example case is described as follows.

- **I2C_Address** — Set this byte as 0xAA. Another value can be used as long as it is different from the Client ATSHA204 I2C_Address.
- **SlotConfig for the Master Key Slot.** (i.e. slot 0) — This key is used to generate diversified key, which is used in the authentication process; therefore, the key must be configured to be “No Read or Write permitted” on this slot.
  The SlotConfig for this slot is 0x81 80. See Table 5-1 for more details.

Table 5-1. SlotConfig for the Master Key Slot

SlotConfig	Comments
ReadKey	Can be set to any value other than zero to avoid the CheckMac copy operation, i.e. 0x1.
CheckOnly	Must be set to zero to enable all crypto functions on this slot.
SingleUse	Must be set to zero to disable the limited usage.
EncryptRead	Must be set to zero to disable read in encryption mode.
IsSecret	Must be set to one to disable read in clear text mode.
WriteKey	Can be set to any value, i.e. 0x0.
WriteConfig	Must be set to disable Write and DeriveKey command, i.e. 0x8.

- **SlotConfig for the Diversified Key Slot** (i.e. slot 1) — Used to check the authenticity of the accessory. The key must be configured to be *No Read*, while the content can only be modified by deriving from Master Key. The SlotConfig for this slot is 0x91 30.

Table 5-2. SlotConfig for the Diversified Key Slot

SlotConfig	Comments
ReadKey:	Can be set to any value other than zero to avoid the CheckMac copy operation, i.e. 0x1.
CheckOnly:	Must be set to one, since it is only used for performing authentication with the accessory.
SingleUse:	Must be set to zero to disable the limited usage.
EncryptRead:	Must be set to zero to disable read in encryption mode.
IsSecret:	Must be set to one to disable read in clear text mode.
WriteKey:	Must be set to Master Key, in this case, 0x0.
WriteConfig:	Can be set to 0x3 or 0xB depends on the authorization is required or not, in this example, it is set to 0x3.

- Other settings can be left as default.

5.1.2 Client ATSHA204 Personalization

The personalization of the client for this example case is shown below.

- **I2C_Address** — Set this byte as 0xBB. Other value can be used as long as it is different from the Host ATSHA204 I2C_address.
- **SlotConfig for the Diversified Key Slot** (i.e. slot 0) — Used to generate response for the authentication process. The key must be configured to be “No Read or Write permitted” on this slot.
  The SlotConfig for this slot is 0x81 80.

Table 5-3. SlotConfig for the Diversified Key Slot

SlotConfig	Comments
ReadKey	Can be set to any value other than zero to avoid the CheckMac copy operation, i.e. 0x1.
CheckOnly	Must be set to zero to enable all crypto functions on this slot.
SingleUse	Must be set to zero to disable the limited usage.
EncryptRead	Must be set to zero to disable read in encryption mode.
IsSecret	Must be set to one to disable read in clear text mode.
WriteKey	Can be set to any value, i.e. 0x0.
WriteConfig	Must be set to disable Write and DeriveKey command, i.e. 0x8.

- Other settings can be left as default.

5.2 Consumable Authentication Use Case

In this case, ATSHA204 is used to authenticate a consumable, track the consumable uses, and also limit the consumable uses. ATSHA204 is embedded in the Host and also in the consumable. In this example, the communication protocol being used is SWI interface.

5.2.1 Host ATSHA204 Personalization

The personalization of the Host for this example case is described below.

- **SelectorMode** — Can be set to any value other than zero to prevent further modification of Selector byte.
- **Slotconfig for the Authentication Key Slot** (i.e. slot 0) — Used to check the authenticity of the consumable. The key must be configured to be “No Read or Write permitted” on this slot.
  The SlotConfig for this slot is 0x91 80. See Table 5-4 for details.

Table 5-4. Slotconfig for the Authentication Key Slot

SlotConfig	Comments
ReadKey	Can be set to any value other than zero to avoid the CheckMac copy operation, i.e. 0x1.
CheckOnly	Must be set to one to enable only CheckMac command.
SingleUse	Must be set to zero to disable the limited usage.
EncryptRead	Must be set to zero to disable read in encryption mode.
IsSecret	Must be set to one to disable read in clear text mode.
WriteKey	Can be set to any value, i.e. 0x0.
WriteConfig	Must be set to disable Write and DeriveKey command, i.e. 0x8.

- **Selector** — Set this byte as 0xAA. Other value can be used as long as it is different from the Client ATSHA204 Selector byte. Value 0x00 is prohibited to prevent further modification on this byte.
- Other settings can be left as default.

5.2.2 Client ATSHA204 Personalization

The personalization of the Host for this example case is described below.

- **SelectorMode** — Can be set to any value other than zero to prevent further modification of Selector byte.
- **SlotConfig for the Authentication Key Slot** — Must use Slot15. Used to generate the response for the authentication process. The key must be configured to be “No Read or Write permitted” on this slot and also configured to be used for a limited use only, i.e. 64 uses.
  The SlotConfig for this slot is 0xA1 80. See Table 5-5 for details.

Table 5-5. SlotConfig for the Authentication Key Slot

SlotConfig	Comments
ReadKey	Can be set to any value other than zero to avoid the CheckMac copy operation, i.e. 0x1.
CheckOnly	Must be set to zero to enable all crypto functions on this slot.
SingleUse	Must be set to one to enable the limited usage.
EncryptRead	Must be set to zero to disable read in encryption mode.
IsSecret	Must be set to one to disable read in clear text mode.
WriteKey	Can be set to any value, i.e. 0x0.
WriteConfig	Must be set to disable Write and DeriveKey command, i.e. 0x8.

- **LastKeyUse** — Set these bytes to 0x00 00 00 00 FF FF FF FF FF FF FF FF. These bytes limit the usage of KeyID 15 to 64 uses.
- **Selector** — Set this byte as 0xBB. Other value can be used as long as it is different from the Host ATSHA204 Selector byte. Value 0x00 is prohibited to prevent further modification on this byte.
- Other settings can be left as default.

6. Revision History

Doc. Rev.	Date	Comments
8845B	05/2013	Simplified the document and added another example.
8845A	11/2011	Initial document release.

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