Application Note

Factory Default Test Data

Atmel ATSHA204

Description

The Atmel® ATSHA204 comes with a preset factory configuration for the Configuration zone and the Data/OTP zones. The factory configuration is intended to be used for constant/fixed vector testing; however, it can also be used as a guide for the customer to configure their own system as many common use cases of the ATSHA204 are covered.

It is *not* recommended that factory values be left in the data key slots. The customer should *always* create unique 32-byte values for these slots prior to system shipment. See the related application note, “Atmel ATSHA204 ACES Walkthrough — Random Secrets*”*.

This application note provides the factory configuration values for the Configuration and Data/OTP zones. These default values are specific to ATSHA204 with RevNum 0x 00 04 05 00. For devices with RevNum other than this, the default values may be different.

The details of the factory Configuration zone, OTP, and key values are discussed.

1. Configuration Zone

The Configuration zone consists of fixed data (serial number and revision number), device configuration (I^2C address, Selector mode, etc.), and slot configuration information. This zone must be written and locked prior to writing to the Data/OTP zones.

1.1 Fixed Data and Device Configuration

Table 1-1. Configuration Zone

Byte #	Name	Description	Default
0:1	SN[0:1]	Part of the serial number value. The values of these bits are fixed at manufacturing time.	0x 01 23
2:3	SN[2:3]	Part of the serial number value. The values of these bits are programmed by Atmel during the manufacturing process and are unique for every die.	—
4:7	RevNum	Chip revision number. Four bytes of information that are used by Atmel to provide manufacturing revision number,	0x 00 04 05 00
8:11	SN[4:7]	Part of the serial number value. The values of these bits are programmed by Atmel during the manufacturing process and are unique for every die.	—
12	SN[8]	Part of the serial number value. The values of these bits are fixed at manufacturing time.	0x EE
13	Reserved	Set by Atmel.	0x 55
14	I2C_Enable	This byte specifies which type interface is enabled on the device. (SWI or I2C).	0x 00 for SWI 0x 01 for I2C
15	Reserved	Set by Atmel.	0x FF
16	I2C_Address	Address for I^2C interface (only relevant for I^2C interface).	0x C8
17	RFU	Reserved for future use. Must be written to 0x00.	0x 00
18	OTPmode	OTP can be set to Read-only mode (0xAA), Consumption mode (0x55), or Legacy Mode (0x00).	0x 55
19	SelectorMode	This byte determines the permission for writing Selector byte.	0x 00
20:51	SlotConfig	Each slot is controlled by two bytes of these bytes. See Section 1.2.	—
52, 54, 56, 58, 60, 62, 64, 66	UseFlag	This byte indicates how many times a key may be used before it is disabled. Each byte corresponds with a single slot. Applies only to keys 0 – 7.	0x FF
53, 55, 57, 59, 61, 63, 65, 67	UpdateCount	For keys that can be updated with DeriveKey. These bytes indicate how many times this operation has been performed. Each byte corresponds with a single slot. Applies to only to keys 0 – 7.	0x 00
68:83	LastKeyUse	These bytes control limited use for KeyID 15.	0x FF
84	UserExtra	This byte is used as an extra byte that can only be updated once if the current value is 0x00.	0x 00
85	Selector	This byte is used as chip ID when executing Pause command.	0x 00
86	LockValue	This byte indicates the lock status of Data/OTP zones.	0x 55
87	LockConfig	This byte indicates the lock status of Configuration zone.	0x 55

1.2 Slot Configuration

Each of the 16 slots in the ATSHA204 device must be configured via the SlotConfig field to control access and usage. Table 1-2 below lists the default values for these fields.

Table 1-2. Slot Configuration

Key	ReadKey	CheckOnly	SingleUse	EncryptRd	IsSecret	WriteKey	WriteConfig	SlotConfig Hex Value
0	15	0	0	0	1	0	Never	0x808F
1	0	0	0	0	1	1	RollAuth	0XA180
2	2	0	0	0	1	0	RollParent	0XE082
3	3	0	1	0	1	0	RollFree	0X60A3
4	4	1	0	0	1	0	Encrypt	0X4094
5	0	0	1	0	1	5	Never	0X85A0
6	6	0	0	0	1	0	Encrypt	0X4086
7	7	0	0	0	1	7	Always	0X0787
8	15	0	0	0	0	0	Always	0X000F
9	9	0	0	0	1	2	ChildAuth	0XF289
10	10	0	0	0	1	10	ChildFree	0X7A8A
11	11	0	0	0	0	11	Never	0X8B0B
12	12	0	0	0	0	12	Encrypt	0X4C0C
13	13	1	0	1	1	13	Encrypt	0X4DDD
14	2	0	0	1	1	2	Encrypt	0X42C2
15	15	0	1	0	1	15	Never	0X8FAF

1.3 Typical Usage

Table 1-3. Typical Slot Usage

Slot #	Typical Usage Description
0	Suitable for a straightforward usage of a fixed key that is the same in all Client devices.
1	Suitable for authentication. Configured as a rollable key — A MAC is required for update, computed using the current value of the key.
2	Suitable for authentication. Configured as a rollable key — A MAC is required, computed using the value stored in a parent slot.
3	Suitable for limited-use (consumable) applications. Configured as a rollable key — no MAC is required for the update.
4	Suitable for a key that is used in the Host device for authentication purpose only.
5	Suitable for a limited or single use mutual authentication.
6	Suitable for applications where the key needs to be updated by using knowledge of another key.
7	Suitable for applications that need an ephemeral or temporary key which can freely be written but never read.
8	Suitable for standard EEPROM replacement where anyone can read and write the slot freely.
9	Suitable for applications that require generation of a unique key in every Client. This key can be generated using the current value in the parent Slot 2.
10	Not a suitable configuration.
11	Suitable for storing read-only data such as product information, model numbers, revision numbers, calibration, etc.
12	Suitable for applications where optional features that must be enabled by an authorizing entity can be done. Configured as a protected write, open read of the data.
13	Suitable for a key that is used in the Host device for authentication purpose only and which can be updated with knowledge of the current value.
14	Suitable for storing confidential field data or as a key that can be recovered and updated at a later time. Configured as R/W encrypted data.
15	Suitable for limited use applications in which the key can be used only up to 128 times.

2. Data/OTP Zones

The ATSHA204 device also comes with preconfigured Data and OTP zones. Each byte on the OTP zone is configured to 0xFF, while each byte on the Data zone is configured with a default specific value. The default value of the ATSHA204 Data zone can be found in Table 2-1. Before writing to the OTP/Data slots, the Configuration zone *must* be configured and locked.

Table 2-1. Data Zones

Slot	Key Value (Hex)
Key 0	00 00 A1 AC 57 FF 40 4E 45 D4 04 01 BD 0E D3 C6 73 D3 B7 B8 2D 85 D9 F3 13 B5 5E DA 3D 94 00 00
Key 1	11 11 23 B6 CC 53 B7 B9 E9 BB 51 FD 2F 74 CD 0E 91 D9 7F EB 84 7B 98 09 F4 CD 93 6A B6 48 11 11
Key 2	22 22 C1 7C 1C 4D 56 89 AA 00 43 E3 9C FB 6B 0B 68 49 E3 2C 24 A3 1B 06 34 49 1E 90 6B 62 22 22
Key 3	33 33 33 61 4A 17 9A 23 6C 7F E4 BE 2F 13 20 67 90 3D B5 1C 72 E0 C9 31 29 6D F4 5A 3E 44 33 33
Key 4	44 44 91 18 68 3D B8 D3 F8 57 0C 74 2E DA DA 52 88 87 30 A5 09 18 54 56 C9 A1 72 38 CF 3C 44 44
Key 5	55 55 86 F2 B3 20 98 A6 E1 E6 33 7A 52 01 03 6A 0D B5 04 02 02 1C 55 B2 57 DF 0C 73 5F 05 55 55
Key 6	66 66 D0 45 3A C2 25 57 F6 D4 6B 7D DF 96 89 DA 2C BC D9 C3 5A D5 9A 42 DE 30 32 CD 25 FC 66 66
Key 7	77 77 2F 4A 9C C0 5E 45 99 BD 26 96 DD 49 F8 A5 06 C8 B6 39 CD 3D A8 4C C6 D1 3C 32 CA 0F 77 77
Key 8	88 88 C6 2A FE 1F 82 D4 E0 85 85 34 4D 77 B8 9D EC 36 F2 06 27 E4 F0 CF 03 0E 27 B8 EE E3 88 88
Key 9	99 99 4E 6D 4A F5 92 30 6B D2 D5 27 7D 77 B3 95 E3 C3 50 8C DA E0 98 1F 9D 28 17 98 8D F4 99 99
Key 10	AA AA 15 A2 55 0B D2 EA 9A F2 96 46 15 69 11 12 96 12 F6 F7 29 FD 50 7C 9A A2 67 92 A1 44 AA AA
Key 11	BB BB 24 DB 78 A8 70 64 A1 F0 8D C9 17 96 60 0A FF 62 D4 C4 4C 3E 10 20 2A AA 8F EC B6 8A BB BB
Key 12	CC CC C6 17 1A 52 45 AC D2 92 46 28 90 62 4C A5 66 2B 22 BB D1 95 DA 2A 9E 49 B8 08 85 0D CC CC
Key 13	DD DD BF AC 11 70 55 9C C9 B6 28 0F 92 95 DF 30 0D EA 22 A0 65 4E 21 C9 CE 74 10 5A 65 D2 DD DD
Key 14	EE EE 08 55 77 BD A7 B8 A7 AF 58 D1 8B 92 F0 DF 79 AD 05 5E 42 82 E9 42 1E D1 3D 7B BD 2E EE EE
Key 15	FF FF 68 B7 B8 01 BE 66 2C EC 74 68 0F E4 7D C1 C6 72 54 3A E5 BE DA 2E 91 9A E5 0D 32 A1 FF FF

3. Revision History

Doc. Rev.	Date	Comments
8842A	11/2012	Initial document release.

Atmel | Enabling Unlimited Possibilities®

Atmel Corporation
1600 Technology Drive
San Jose, CA 95110
USA
Tel: (+1) (408) 441-0311
Fax: (+1) (408) 487-2600
www.atmel.com

Atmel Asia Limited
Unit 01-5 & 16, 19F
BEA Tower, Millennium City 5
418 Kwun Tong Roa
Kwun Tong, Kowloon
HONG KONG
Tel: (+852) 2245-6100
Fax: (+852) 2722-1369

Atmel Munich GmbH
Business Campus
Parkring 4
D-85748 Garching b. Munich
GERMANY
Tel: (+49) 89-31970-0
Fax: (+49) 89-3194621

Atmel Japan G.K.
16F Shin-Osaki Kangyo Bldg
1-6-4 Osaki, Shinagawa-ku
Tokyo 141-0032
JAPAN
Tel: (+81) (3) 6417-0300
Fax: (+81) (3) 6417-0370