APPLICATION NOTE

Authentication Counting

Atmel CryptoAuthentication

Features

- How to achieve high endurance counters in excess of 800,000 counts.
- How to disable the Atmel® CryptoAuthentication™ ATSHA204A device after a pre-set number of authentications.
  - Device Configuration
  - System Software Operations
- How to count the number of authentications with the ATSHA204A.
  - Device Configuration
  - System Software Operations
- Applications applies to the Atmel CryptoAuthentication Devices:
  - ATSHA204(A)
  - ATECC108(A)
  - ATECC508A

Introduction

With many consumable applications, there is a requirement to limit the number authentications that can be performed on a slot. The limited use capability of Slot F can be used if the total number of authentications is not greater than 128. To track the number of authentications beyond 128, the technique of chaining SingleUse slots can be used. This is made possible since the DeriveKey command on slot numbers up to Slot 8 resets the UseFlag to FF. When Slot F is the last slot in the authentication chain, this technique limits the use of the device. This example will chain Slots 7 to F.

Sometimes, only high endurance counting is required. To support applications where the number of authentications is the only thing of interest without a requirement for authentications to be limited, chaining SingleUse slots can be used. When the last slot in the chain is also derivable and the rolling UpdateCount is kept tracked, a rolling authentication counter can be achieved.

Table of Contents

1 Authentication Consumption by Chaining SingleUse Slots 3

1.1 Slot Configuration 3

1.2 Consumption Tracking 3

1.3 Consumption Chaining Examples 4

2 Authentication Counter by Chaining SingleUse Slots 5

2.1 Slot Configuration 5

2.2 Authentication Counting 6

2.3 Authentication Counting Examples 7

3 Revision History 7

1 Authentication Consumption by Chaining SingleUse Slots

With many consumable applications, there is a requirement to limit the number authentications that can be performed on a slot. Slot F's limited use capability can be used if the total number of authentications is not greater than 128. To track the number of authentications beyond 128, the technique of chaining single use slots can be used. This is made possible since the `DeriveKey` command on slot numbers less than eight resets the UseFlag to FF. When Slot F is the last slot in the authentication chain, this technique limits the use of the device. This example will chain Slots 7 and F.

1.1 Slot Configuration

The slot configurations are as follows:

Table 1-1. Slot Configuration

Slot	Description
7	SlotConfig Bytes: AF 3F ReadConfig: AF (1010 1111), IsSecret, SingleUse WriteConfig: 3F (0011 1111), DeriveKey, Use Parent, No Authorizing MAC, WriteKey=F Key: Initialize to the result of DeriveKey.
F	SlotConfig Bytes: AF 8F ReadConfig: AF (1010 1111), IsSecret, SingleUse WriteConfig: 8F (1000 1111), IsSecret

Use Slot 7 as the primary authentication slot with either the Fixed-Challenge sequence or the Random-Challenge authentication sequence. Either authentication will consume one UseFlag bit per authentication.

1.2 Consumption Tracking

Table 1-2. Consumption Timing

Step	To ATSHA204A	System Software
1	MAC or CheckMac Authentication	
2	Read(UseFlag Slot 7)	
3		If UseFlag is not zero, then do nothing further.
4		If UseFlag is zero, continue.
5	Nonce(Fixed)	
6	DeriveKey(Slot 7)	

Notes:
1. Step 1: Consume one UseFlag bit.
2. Steps 2 thru 4: Check to see if the UseFlag is used up.
3. Step 5: Use the same constant value for the Nonce.
4. Step 6: Initiate a DeriveKey.
    - The same key is in Slot 7 after DeriveKey.
    - Reset UseFlag in Slots 7 to FF.
    - Consume one LastKeyUse for Slot F.

The equation that determines the number of authentications is as follows:

Number of Authentications:

$$\#auths = \sum \left(8^{(n-1)} C_n\right) + 8^n (C_{LKU})$$

Where: n = The number of chained slots.

C_n = The count of UseFlag$_n$ bits consumed = 8 max (for Slots 0 to 7)

C_{LKU} = The count of LastKeyUse bits consumed = 128 max

1.3 Consumption Chaining Examples

Use the table below to determine the number of chained slots for your application.

Examples:

$$n = 1$$
$$\#auths = C_1 + 8(C_{LKU})$$

$$n = 2$$
$$\#auths = C_1 + 8C_2 + 64(C_{LKU})$$

The number of authentications that is possible when linking in this way is shown in the following table.

Table 1-3. Possible Authentications When Linking

Chaining (n)	Auth Calculation	#Auths Max	1st Slot Endurance Count[1]	Notes
1 SingleUse to Slot F	$8 + (8^1 \times 128)$	1,032	129	
2 SingleUse to Slot F	$8 + (8^1 \times 8) + (8^2 \times 128)$	8,264	1,033	
3 SingleUse to Slot F	$8 + (8^1 \times 8) + (8^2 \times 8) + (8^3 \times 128)$	66,120	8,265	
4 SingleUse to Slot F	$8 + (8^1 \times 8) + (8^2 \times 8) + (8^3 \times 8) + (8^4 \times 128)$	528,968	66,121	Maximum recommended number of slots to chain together is “4” due to EE wear.
5 SingleUse to Slot F	$8 + (8^1 \times 8) + (8^2 \times 8) + (8^3 \times 8) + (8^4 \times 8) + (8^5 \times 128)$	4,231,752	528,969	Maximum recommendation of 800,000 authentications instead of 4,231,752 to stay within the limit of the first slot EE endurance.[1]

Note: 1. EEPROM Endurance is 100,000 maximum.

2 Authentication Counter by Chaining SingleUse Slots

Sometimes, only high endurance counting is required. To support applications where the number of authentications is the only thing of interest without a requirement for authentications to be limited, chaining SingleUse slots can be used. When the last slot in the chain is also derivable and the rolling UpdateCount is kept tracked, a rolling authentication counter can be achieved.

2.1 Slot Configuration

This example will chain Slots 6, 7, and 8. The slot configurations are as follows:

Table 2-1. Slot Configuration

Slot	Description	
6	SlotConfig Bytes: ReadConfig: WriteConfig:	AF 37 AF (1010 1111), IsSecret, SingleUse 36 (0011 0111), DeriveKey, Use Parent, No Authorizing MAC, WriteKey=7
7	SlotConfig Bytes: ReadConfig: WriteConfig:	AF 38 AF (1010 1111), IsSecret, SingleUse 37 (0011 1000), DeriveKey, Use Parent, No Authorizing MAC, WriteKey=8
8	SlotConfig Bytes: ReadConfig: WriteConfig:	8F 8F AF (1000 1111), IsSecret 8F (1000 1111), IsSecret

Use Slot 6 as the primary authentication slot with either the Fixed Challenge sequence or the Random Challenge authentication sequence. Either authentication will consume one UseFlag bit per authentication.

2.2 Authentication Counting

Table 2-2. Consumption Tracking

Step	To ATSHA204A	System Software
1	MAC or CheckMac Authentication	
2	Read(UseFlag slot 6)	
3		If UseFlag is not zero, then do nothing further.
4		If UseFlag is zero, continue.
5	Nonce(Fixed)	
6	DeriveKey(slot 6)	
6	Read(UseFlag slot 6)	
7		If UseFlag is not zero, then do nothing further.
8		If UseFlag is zero, continue.
9	Nonce(Fixed)	
10	DeriveKey(slot 7)	
11	Read(UpdateCount slot 7)	

1. Step 1: Consume one UseFlag bit.
2. Steps 2 thru 4: Check to see if the UseFlag is used up.
3. Step 5: Initiate a DeriveKey on Slot 6.
   - Reset UseFlag in Slot 6 to FF.
   - UpdateCount in Slot 6 is incremented (rolls to zero after FF).
   - Consume one UseFlag for Slot 7.
   - DeriveKey
4. Steps 6 thru 8: Check to see if the UseFlag is used up.
5. Step 5: Initiate a DeriveKey on Slot 7.
   - Reset UseFlag in Slot 7 to FF.
   - UpdateCount in Slot 7 is incremented (rolls to zero after FF).

The equation that determines the number of authentications is as follows:

Number of Authentications:

$$\#auths \; = \; \sum \left(8^{(n-1)}C_n\right) \; + \; 8^n(UpdateCount_n)$$

Where: n = The number of chained slots.

C_n = The count of UseFlag_n bits consumed = 8 max (for Slots 0 to 7)

$UpdateCount_n$ = The UpdateCount for the slot = 256 max (for Slots 0 to 7)

2.3 Authentication Counting Examples

Use the table below to determine the number of chained slots for the application.

Examples:

$$n = 1$$
$$\#auths = C_1 + 8(UpdateCount_1)$$

$$n = 2$$
$$\#auths = C_1 + 8C_2 + 64(UpdateCount_2)$$

$$n = 3$$
$$\#auths = C_1 + 8C_2 + 64C_3 + 512(UpdateCount_3)$$

The number of authentications that is possible before rolling the counter is shown in the following table.

Table 2-3. Possible Authentications Before Rolling the Counter

Chaining	Auth Calculation	#Auths Max	1st Slot Endurance Count	Notes
1 SingleUse Chained	8 + (8^1 x 256)	2,056	257	
2 SingleUse Chained	8 + (8^1 x 8) + (8^2 x 256)	16,456	2,057	
3 SingleUse Chained	8 + (8^1 x 8) + (8^2 x 8) + (8^3 x 256)	131,656	16,457	Maximum recommended number of slots to chain together is “3” due to EE wear.
4 SingleUse Chained	8 + (8^1 x 8) + (8^2 x 8) + (8^3 x 8) + (8^4 x 256)	1,053,256	131,657	Maximum recommendation of 800,000 authentications instead of 1,053,256 to stay within the limit of the first slot EE endurance.

Note: 1. EEPROM Endurance is 100,000 maximum.

3 Revision History

Doc Rev.	Date	Comments
8863A	04/2015	Initial document release.

Atmel | 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.

SAFETY-CRITICAL, MILITARY, AND AUTOMOTIVE APPLICATIONS DISCLAIMER: Atmel products are not designed for and will not be used in connection with any applications where the failure of such products would reasonably be expected to result in significant personal injury or death (“Safety-Critical Applications”) without an Atmel officer's specific written consent. Safety-Critical Applications include, without limitation, life support devices and systems, equipment or systems for the operation of nuclear facilities and weapons systems. Atmel products are not designed nor intended for use in military or aerospace applications or environments unless specifically designated by Atmel as military-grade. Atmel products are not designed nor intended for use in automotive applications unless specifically designated by Atmel as automotive-grade.