# AN4206

# Authenticating Consumables with the ATSHA204A and PIC16 Microcontroller


*Authors:* *Bill Hawkins*
*Zhang Feng*
*Xavier Bignalet*
*Microchip Technology Inc.*


## INTRODUCTION

The authentication of a consumable component is a common requirement in many familiar systems. Examples include ink cartridges in printers, batteries in vehicles, cosmetic product cartridges, and medications in drug-delivery devices. This document examines the benefits of incorporating Microchip's ATSHA204A secure element from the CryptoAuthentication™ family into an existing design to allow the secure authentication of consumables. See Figure 1.

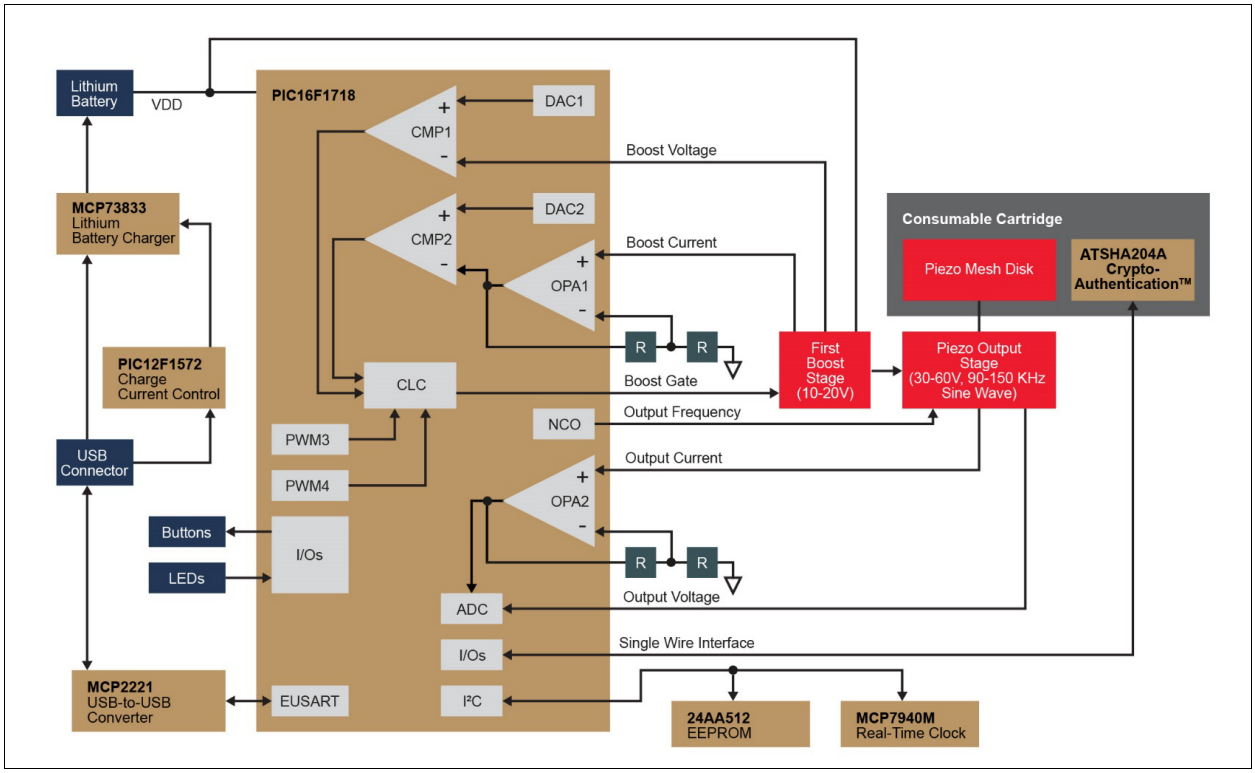
For this example, we will start with Microchip's AN2265, "*Vibrating Mesh Nebulizer Reference Design*" (DS00002265) which describes a vibrating mesh nebulizer and how it can be implemented with Microchip's Core-Independent Peripherals. This document describes how updating the nebulizer reference design to include secure authentication of the removable vibrating mesh and medicine tank cartridge enhances the design.

The nebulizer reference design has a removable cartridge that holds the mesh which will wear over time, and the supply of medicine which is a consumable material supply. This removable cartridge that holds the medicine can greatly affect the performance of the device.

Manufacturers may want to protect these cartridge applications against third-party suppliers for several reasons as follows:

- The customer's impression of the quality and function of the device is strongly influenced by the substance inside the cartridge. When a third-party replacement does not meet the manufacturer's standards and also gives inferior performance not meeting the customer's expectation, the manufacturer receives the complaints not the third-party cartridge.

**FIGURE 1: SECURE AUTHENTICATED NEBULIZER BLOCK DIAGRAM**



- Especially in the medical industry, allowing uncontrolled access to the device may expose the manufacturer to liability for treatment with the wrong dosage, contaminated medicine, or even the wrong medicine in a consumable cartridge.
- Another reason is for protection of the revenue stream. A typical business model includes the expectation that sales of consumable supplies will provide the main revenue stream to support the company. If a third party can sell into the same market, this deprives the manufacturer of the revenue that it should be getting to recoup costs of the base unit and Research and development (R&D).

This document describes the security enhancements made to the nebulizer to authenticate the removable cartridge, track its use, and potentially limit the usage of the cartridge to prevent problems with wear out of the hardware, and unauthorized refilling and reuse of an old cartridge.

## INTRODUCING THE ATSHA204A

The nebulizer uses a ATSHA204A chip on the cartridge to authenticate the cartridge to the base unit. The ATSHA204A has several features that are used to enable authentication, such as SHA-256 hash algorithm, secure EEPROM, unique serial number, high-quality random number generator, and $I^2C$ interface or a single wire interface.

### SHA-256 Cryptography Engine

The ATSHA204A integrates a SHA-256 hash algorithm in hardware. This hash function takes an input stream (the challenge) and produces a 256-bit (32 byte) output (the response). The two main properties of the hash functions are as follows:

- It is not feasible to reproduce the input stream from the hashed output.
- It is not feasible to alter the input stream and get the same hash output.

The ATSHA204A will hash a secret key with a challenge string provided from the host microcontroller. The microcontroller can also perform the hash function with that challenge string and the secret key. If the hashed output matches what the host microcontroller expects, then it proves that the ATSHA204A device knows the same secret key.

### Secure EEPROM/Key Storage

The ATSHA204A has 512 bytes of EEPROM arranged in sixteen 32 byte slots. Any of these slots may be configured as a key value to be used in the hash function. When the ATSHA204A is configured, the values in the slots may be write protected, read protected, encrypted with another slot as a key, or left as readable/writeable EEPROM locations. There are physical anti-tamper and side channel protections to prevent someone from decapping and probing the die of the device to read out the memory.

### Unique Serial Number

Each ATSHA204A is guaranteed to have a unique 72-bit (9 byte) serial number, which allows the manufacturer to uniquely identify any device with the ATSHA204A attached.

### High-Quality Random Number Generator

The ATSHA204A has a high-quality random number generator based on noise source. This can be used to create unique challenges that will only be used one time and prevents an attacking device from recording challenge and response to play back to the host to impersonate a valid device.

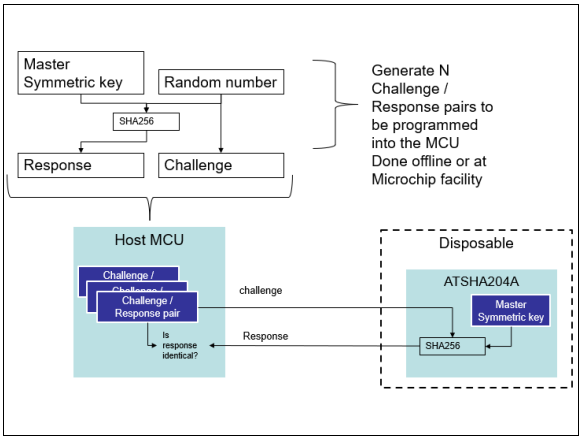
### $I^2C$/Single Wire Interface

The ATSHA204A is available with either an $I^2C$ interface or a single wire interface that allows the cartridge to have the minimum number of contacts in the interface. The authenticated nebulizer uses the single wire interface with a chip package that has three large pads. The ATSHA204A chip is meant to be glued to the cartridge, and then the host just supplies wiping contacts to connect to the cartridge (like a battery connector), such that there is no board or mating connector required for the cartridge.

## HOW IS THE ATSHA204A USED FOR AUTHENTICATION?

The secure nebulizer demo is a single chip system design. A PIC16F1718 runs the entire operation including the challenge/response for the authentication with the ATSHA204A. See Figure 2.

**FIGURE 2: ATSHA204A AUTHENTICATION BLOCK DIAGRAM**

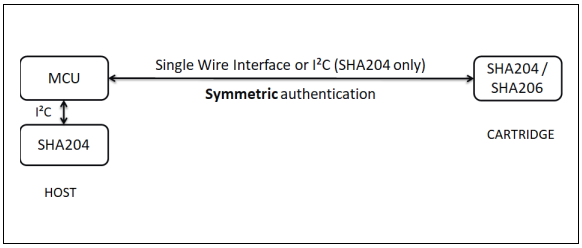


The PIC16 has 16 challenge/response pairs stored in memory. The cartridge is authenticated every time the device is used. When the user presses the button to start the nebulizer, the PIC16 host sends a 32 byte challenge to the ATSHA204A on the cartridge. The ATSHA204A then hashes the challenge with the secret key and returns that value to the PIC16. The value returned is compared with the expected response, and if they match, then the nebulizer is allowed to run. If they do not match, then the nebulizer turns on a red LED for a few seconds, then shuts off. The nebulizer could choose from these 16 challenges more or less unpredictably by using the lower 4 bits in a free-running timer to pick which one to use.

Because the PIC16 stores a limited number of challenge/response pairs, this would imply that a clone device would only need to handle a limited number cases to defeat the security of this system. To prevent this from happening, each PIC16 host can be programmed with unique challenge/response pairs, so that a clone created in this manner would not work on any other devices.

The authentication method protects the accessory/disposable, but does not prevent cloning the Host (copy of the Challenge/response pair in a new system). A higher level of security would be to add a separate secure element (ATSHA204A) next to Host MCU. See Figure 3. This Host ATSHA204A could generate random challenge for the cartridge ATSHA204A and provide a response to compare with the response from the cartridge ATSHA204A. Furthermore, a Key Derivation implementation would further improve the robustness of the solution.

**FIGURE 3: SYMMETRIC AUTHENTICATION**




Alternatively to the ATSHA204A, the ATSHA206A becomes the ideal solution when the form factor mandate the usage of a 2-pin only package due to the confined size of the cartridge that cannot allow for any PCB. The 2-pin ATSHA206A or 3-pin ATSHA204A can be molded inside the disposable cartridge. An integrated capacitor is added inside the ATSHA206A providing parasitic power capability on the supply pin. Essentially the data and the power are sharing the same pin.

## LIMITING USAGE OF THE CARTRIDGE

The authenticated nebulizer keeps a usage count for each cartridge. This data can be used to limit use of the cartridge. There are a couple of mechanisms to implement this feature.

ATSHA204A device contains EEPROM and SRAM two memory blocks. The EEPROM is divided into three zones: Data, Configuration, and One-Time-Programmable (OTP).

Data zone splits into 16 general purpose memory slots. Any slot in the Data zone of the EEPROM can be used to store a key.

There are 128 bits in the Configuration zone assigned as LastKeyUse which is used to limit the usage of key number 15 stored at Slot 15. These 128 bits get cleared on each use of Slot 15 as a key. There is no reset mechanism. The Slot/Key 15 is permanently disabled after 128 uses. Therefore, the usage count for each cartridge can be limited to 128 times or less.

There are also 512 bits of OTP memory that can be used to store read-only data or one-way fuse type consumption logging information. When configured in Consumption mode, bits can be written to '0', but never written back to a '1'. Therefore, a '0' can be shifted to the OTP memory 512 times before the OTP memory is all zeros. The usage of the cartridge can be blocked after the OTP memory is all zeroes.

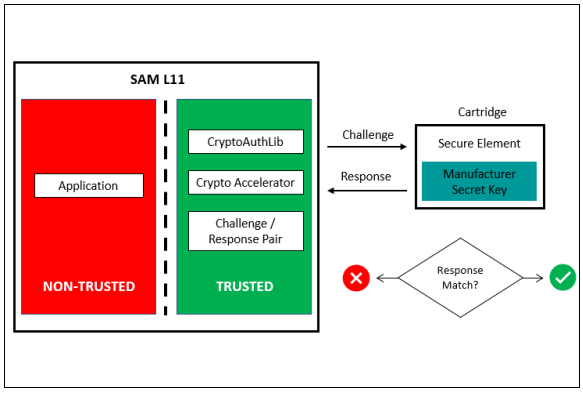
If the usage of the cartridge is less than these values (128 times for Slot 15, or 512 times for OTP), then some of these bits can be preprogramed to zeros, such that the necessary number of ones are available for the required usage.

## FURTHER SECURITY ENHANCEMENTS DISCUSSION

Secret keys stored in the host MCU, the ATSHA204A or computer system of the company, must absolutely be protected. If the key leaks out, then there would be no more security, and products can be cloned easily.

Some of Microchip's 32-bit microcontrollers with robust security provide trusted execution environment (TEE), crypto accelerators, secure boot, secure bootloader, and so on. For example, Figure 4 shows a SAM L11 as the host MCU in the accessory authentication application, where the SAM L11 adds robustness is in hosting TEE the CryptoAuthlib API calls from the MCU to the secure element. The TEE isolate the critical code where the Cryptoauthlib API callbacks would leave from the rest of the system and avoid firmware alteration.

**FIGURE 4: AUTHENTICATION OF DISPOSABLE CARTRIDGES**




Keys of the disposable cartridge that are stored in the ATSHA204A are safe from prying eyes. The ATSHA204A is only one choice of the security chips offered by Microchip. There are other devices that use Public Key cryptography, which is used in network authentication, to prevent having a single key that can be compromised. Each device will have its own key, and its authenticity is determined by a certificate which provides traceability of the device back to a root authority. The description of those devices is beyond the scope of this document, but more information can be found in the security design center on the Microchip website at:

https://www.microchip.com/design-centers/security-ics

## APPENDIX A: WARNINGS, RESTRICTIONS AND DISCLAMER

Microchip medical reference designs and demos are intended for evaluation and development purposes only. Use of Microchip devices in life support and/or safety applications is entirely at the buyer's risk, and the buyer agrees to defend, indemnify and hold harmless Microchip from any and all damages, claims, suits, or expenses resulting from such use.

## APPENDIX B: REFERENCES

- AN2265, *"Vibrating Mesh Nebulizer Reference Design"* (DS00002265), Bill Hawkins and Zhang Feng, Microchip Technology Inc.
  - See AN2265 from the Microchip product page at: https://www.microchip.com/en-us/solutions/medical/drug-delivery-devices/nebulizer
- ATSHA206A Disposable Cartridges Secure Authentication
  - See ATSHA206A product page at https://www.microchip.com/en-us/product/ATSHA206A

**Note the following details of the code protection feature on Microchip products:**

- Microchip products meet the specifications contained in their particular Microchip Data Sheet.
- Microchip believes that its family of products is secure when used in the intended manner, within operating specifications, and under normal conditions.
- Microchip values and aggressively protects its intellectual property rights. Attempts to breach the code protection features of Microchip product is strictly prohibited and may violate the Digital Millennium Copyright Act.
- Neither Microchip nor any other semiconductor manufacturer can guarantee the security of its code. Code protection does not mean that we are guaranteeing the product is “unbreakable”. Code protection is constantly evolving. Microchip is committed to continuously improving the code protection features of our products.



*For information regarding Microchip’s Quality Management Systems, please visit www.microchip.com/quality.*

**Trademarks**



ISBN: 978-1-5224-8943-6

# Worldwide Sales and Service


## AMERICAS

**Corporate Office**
2355 West Chandler Blvd.
Chandler, AZ 85224-6199
Tel: 480-792-7200
Fax: 480-792-7277
Technical Support:
http://www.microchip.com/support
Web Address:
www.microchip.com

**Atlanta**
Duluth, GA
Tel: 678-957-9614
Fax: 678-957-1455

**Austin, TX**
Tel: 512-257-3370

**Boston**
Westborough, MA
Tel: 774-760-0087
Fax: 774-760-0088

**Chicago**
Itasca, IL
Tel: 630-285-0071
Fax: 630-285-0075

**Dallas**
Addison, TX
Tel: 972-818-7423
Fax: 972-818-2924

**Detroit**
Novi, MI
Tel: 248-848-4000

**Houston, TX**
Tel: 281-894-5983

**Indianapolis**
Noblesville, IN
Tel: 317-773-8323
Fax: 317-773-5453
Tel: 317-536-2380

**Los Angeles**
Mission Viejo, CA
Tel: 949-462-9523
Fax: 949-462-9608
Tel: 951-273-7800

**Raleigh, NC**
Tel: 919-844-7510

**New York, NY**
Tel: 631-435-6000

**San Jose, CA**
Tel: 408-735-9110
Tel: 408-436-4270

**Canada - Toronto**
Tel: 905-695-1980
Fax: 905-695-2078

## ASIA/PACIFIC

**Australia - Sydney**
Tel: 61-2-9868-6733

**China - Beijing**
Tel: 86-10-8569-7000

**China - Chengdu**
Tel: 86-28-8665-5511

**China - Chongqing**
Tel: 86-23-8980-9588

**China - Dongguan**
Tel: 86-769-8702-9880

**China - Guangzhou**
Tel: 86-20-8755-8029

**China - Hangzhou**
Tel: 86-571-8792-8115

**China - Hong Kong SAR**
Tel: 852-2943-5100

**China - Nanjing**
Tel: 86-25-8473-2460

**China - Qingdao**
Tel: 86-532-8502-7355

**China - Shanghai**
Tel: 86-21-3326-8000

**China - Shenyang**
Tel: 86-24-2334-2829

**China - Shenzhen**
Tel: 86-755-8864-2200

**China - Suzhou**
Tel: 86-186-6233-1526

**China - Wuhan**
Tel: 86-27-5980-5300

**China - Xian**
Tel: 86-29-8833-7252

**China - Xiamen**
Tel: 86-592-2388138

**China - Zhuhai**
Tel: 86-756-3210040

## ASIA/PACIFIC

**India - Bangalore**
Tel: 91-80-3090-4444

**India - New Delhi**
Tel: 91-11-4160-8631

**India - Pune**
Tel: 91-20-4121-0141

**Japan - Osaka**
Tel: 81-6-6152-7160

**Japan - Tokyo**
Tel: 81-3-6880- 3770

**Korea - Daegu**
Tel: 82-53-744-4301

**Korea - Seoul**
Tel: 82-2-554-7200

**Malaysia - Kuala Lumpur**
Tel: 60-3-7651-7906

**Malaysia - Penang**
Tel: 60-4-227-8870

**Philippines - Manila**
Tel: 63-2-634-9065

**Singapore**
Tel: 65-6334-8870

**Taiwan - Hsin Chu**
Tel: 886-3-577-8366

**Taiwan - Kaohsiung**
Tel: 886-7-213-7830

**Taiwan - Taipei**
Tel: 886-2-2508-8600

**Thailand - Bangkok**
Tel: 66-2-694-1351

**Vietnam - Ho Chi Minh**
Tel: 84-28-5448-2100

## EUROPE

**Austria - Wels**
Tel: 43-7242-2244-39
Fax: 43-7242-2244-393

**Denmark - Copenhagen**
Tel: 45-4485-5910
Fax: 45-4485-2829

**Finland - Espoo**
Tel: 358-9-4520-820

**France - Paris**
Tel: 33-1-69-53-63-20
Fax: 33-1-69-30-90-79

**Germany - Garching**
Tel: 49-8931-9700

**Germany - Haan**
Tel: 49-2129-3766400

**Germany - Heilbronn**
Tel: 49-7131-72400

**Germany - Karlsruhe**
Tel: 49-721-625370

**Germany - Munich**
Tel: 49-89-627-144-0
Fax: 49-89-627-144-44

**Germany - Rosenheim**
Tel: 49-8031-354-560

**Israel - Ra'anana**
Tel: 972-9-744-7705

**Italy - Milan**
Tel: 39-0331-742611
Fax: 39-0331-466781

**Italy - Padova**
Tel: 39-049-7625286

**Netherlands - Drunen**
Tel: 31-416-690399
Fax: 31-416-690340

**Norway - Trondheim**
Tel: 47-7288-4388

**Poland - Warsaw**
Tel: 48-22-3325737

**Romania - Bucharest**
Tel: 40-21-407-87-50

**Spain - Madrid**
Tel: 34-91-708-08-90
Fax: 34-91-708-08-91

**Sweden - Gothenberg**
Tel: 46-31-704-60-40

**Sweden - Stockholm**
Tel: 46-8-5090-4654

**UK - Wokingham**
Tel: 44-118-921-5800
Fax: 44-118-921-5820