Application Note

Atmel CryptoAuthentication Product Uses

Atmel ATSHA204

Abstract

Companies are continuously searching for ways to protect property using various security implementations; however, the cost of security implementation can drive companies away from effective hardware solutions to less secure software solutions. With the introduction of the Atmel® ATSHA204 CryptoAuthentication™ device, affordable hardware security is readily available and provides exceptional protection.

Overview

ATSHA204 is an exceptional device that enables solutions to countless problems across many industries. Outlined within this document are use cases which provide brief descriptions of the possible ATSHA204 applications and how these applications can be implemented.

1. Accessory Authentication

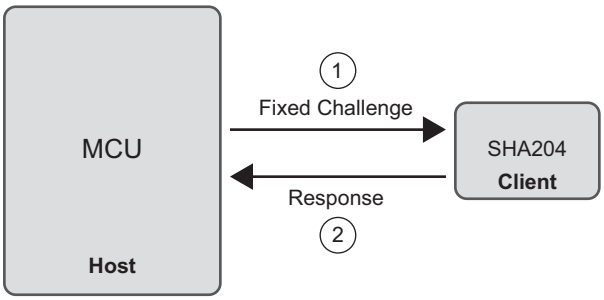
The below Fixed Challenge Response authentication process can be used for a multitude of use cases. For explanation purposes, the Fixed Challenge Response is used in an accessory application.

ATSHA204 CryptoAuthentication can be used for authenticating an accessory. To do the authentication, ATSHA204 should be embedded on the accessory (Client).

The authentication process uses a challenge-response pair selected from a challenge-response pair pool. Before using the accessory, a challenge is sent to ATSHA204 on the Client. The Client then calculates the response and sends the response to the Host. Upon receiving the response, the Host compares it with the expected response. If the responses matched, then the Client is said to be authentic.

By using this configuration, only authentic accessories can be used by the system. The accessory authentication process is illustrated in Figure 1-1.

Figure 1-1. Fixed Challenge Response



Possible applications are listed below:

- Mobile devices — authenticating the battery
- Medical equipment authentication
- Device Accessories, such as earphones, speakers, docking station, chargers, etc.

2. Consumable Authentication

The below, Random Challenge Response authentication process can be used for a multitude of use cases. For explanation purposes, the Random Challenge Response is used in a consumable application.

By embedding the ATSHA204 device into a consumable (Client) and sending a challenge from the system (Host), companies can guarantee that only authentic consumables are used in their systems.

In this scheme, a random challenge is used to authenticate the consumable product. Before using the consumable, the Host is sent a random challenge to the Client. The Client then calculates the response and sends the response to the Host. Upon receiving the response, the Host compares it with the expected response.

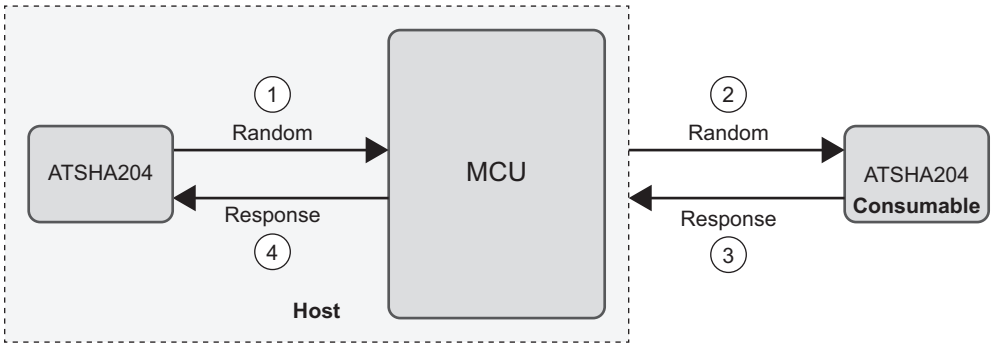
ATSHA204 has a special feature for limiting the usage amount of the consumable attached in the system. ATSHA204 has a special key which can be used only for a limited usage. The usage amount of the key is decreased each time the key is used for performing authentication. After a maximum of 128 uses, the key is permanently disabled. Any further usage of this key will return an error. If higher than 128 counts are required, there is a method to chain slots together. See application note, “Atmel ATSHA204 Chaining of Keys for Consumption”.

To increase the security level, a diversified-key scheme can be used. In this scheme, each ATSHA204 would have an unique key which is diversified based on its serial number. If an accessory is compromised, then it would not affect other accessory because each accessory has each unique key.

An additional level of security can be added to the system by using another ATSHA204 device in the Host. ATSHA204 maintains the secret keys in the hardware instead of embedding them into the Host microprocessor code. This makes the keys irretrievable for hackers attempting to circumvent the system.

Figure 2-1 illustrates an example of the ATSHA204 device use to validate consumables.

Figure 2-1. Random Challenge Response



Using the serial number to implement a key diversification scheme is recommended in order to limit the adverse effects if one of the keys is compromised by failed control processes or corporate espionage. When using a diversified key, the source of compromise can be isolated, and a remedy can be implemented much more rapidly.

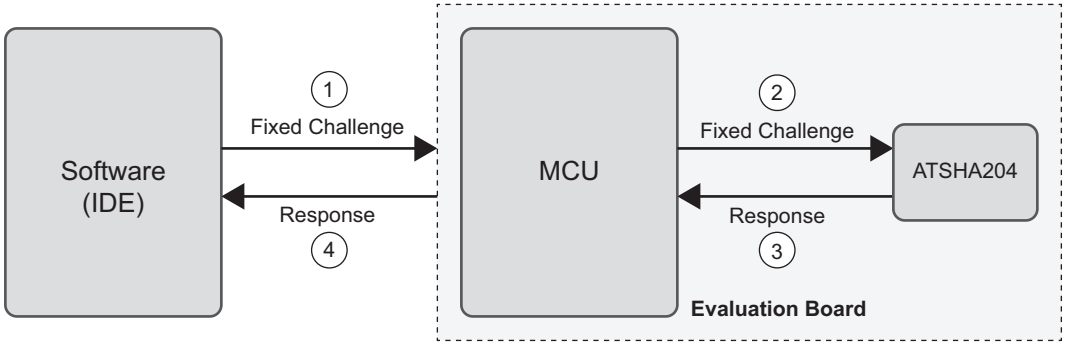
Possible applications for this configuration are:

- Printers — authenticating the cartridge.
- Air Purification — authenticating the filter.

3. System Anti-Cloning/Anti-Piracy

ATSHA204 CryptoAuthentication provides an exceptional method preventing third parties from creating board clones. To implement, the board should be embedded with its own ATSHA204 device. The Integrated Development Environment (IDE) would then be programmed to challenge the board prior to allowing the developer access to it. Counterfeiters will not be able to replicate every possible occurrence of challenge and response that can be handled by a board containing a legitimate CryptoAuthentication device; thereby, thwarting common cloning attempts. Providing a periodic method of renewing challenge-response would increase security by removing any existing compromise as each incremental application upgrade could replace the list of challenge-response pairs. Figure 3-1 illustrates the operation of this security model.

Figure 3-1. Anti-Cloning / Anti-Piracy



Companies may also want to identify authentic boards prior to rendering technical support. An interface could be implemented that would enable the user to enter any string of text that would in turn be fed to the ATSHA204 device on the development board and the response displayed to the user. The help desk operator could verify the system by providing the user a custom string and asking them for the generated response. The help desk operator would then be able to verify the authenticity of the development board prior to rendering service to the customer.

4. Session-Key Exchange

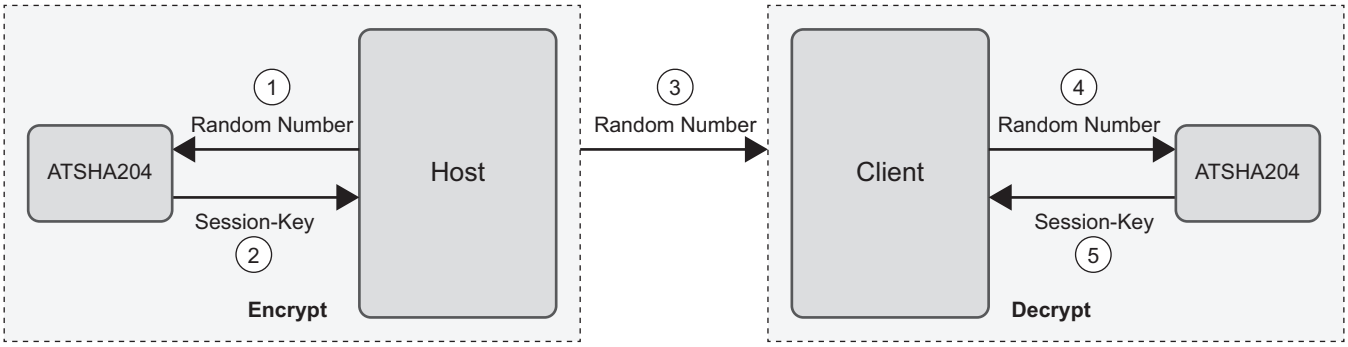
ATSHA204 CryptoAuthentication can also be used for secure key exchange. In this scheme, ATSHA204 is used in conjunction with a symmetric encryption algorithm such as AES or DES. ATSHA204 can facilitate this by using the unique response produced by the device as a key to the symmetric encryption algorithm.

To guarantee the uniqueness of the encryption key, a random number is needed in the generation process. This random number is used to generate unique session key. The random number can be a constant, something related to the current system, or a random number obtained from ATSHA204.

The key exchange is done by sending a random challenge to Host ATSHA204, which generates a response that is used as session-key for encrypting the message. The message and the random challenge are then sent to the client ATSHA204. In the client side, the random challenge is fed into ATSHA204 to generate the response which is used as key to decrypt the message. It should be noted that the key is the root key is the same on both the host and client.

Figure 4-1 illustrates how to encrypt and decrypt multiple files using key generated by ATSHA204.

Figure 4-1. Session Key Exchange Using ATSHA204



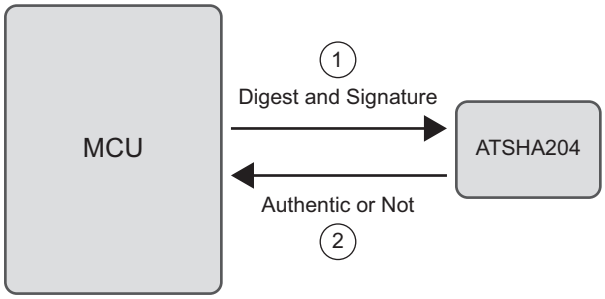
5. Secure Boot

Modern systems are often built using a standard microprocessor with the operating program stored in flash memory. Such architecture can permit the manufacturer to quickly take advantage of advances in processor performance and memory cost while offering fast time to market. If the operating program is stored in an external Flash device, it's very hard to prevent an adversary from obtaining its contents and modifying it to run a fraudulent program. By using ATSHA204 in the system, the manufacturer can ensure that only authentic program can be run on the system.

To implement secure boot, a validating code or signature is stored in flash along with the operating program. As part of the boot program execution at system startup, the security device verifies the signature to ensure that the program is authentic. If the verification succeeds, the operating program is executed and the system operates in the normal way. Any modification of the operating program, even a single bit, will require a new validating signature.

The secure boot scheme is illustrated in Figure 5-1.

Figure 5-1. Secure Boot



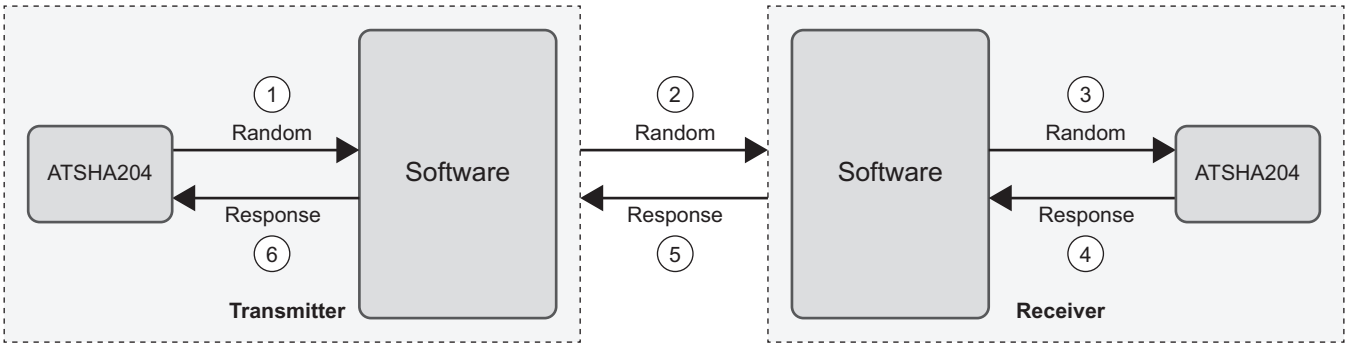
Furthermore, the manufacturer is also able to ensure that only an authentic system can run the program by performing mutual authentication. The mutual authentication is supported by ATSHA204 by using CheckMac copy operation.

6. Network Security

Wireless transmission devices have to verify each node prior to allowing access to the network. ATSHA204 CryptoAuthentication is a great option for offering a low-cost verification method. By installing ATSHA204 devices in the radio nodes (Client), the transmitting node (Host) can verify that it is communicating with valid network nodes before transmitting important commands or information. Additional security can be achieved by adding another ATSHA204 device in the Host so the customer's secrets would not have to be kept in the microprocessor code where developers and subcontractors may have access to them. When using additional ATSHA204 on transmitting node, both ATSHA204 must agree on the same keys value.

Figure 6-1 illustrates a configuration that utilizes two ATSHA204 devices in a radio network.

Figure 6-1. Wireless Node Authentication

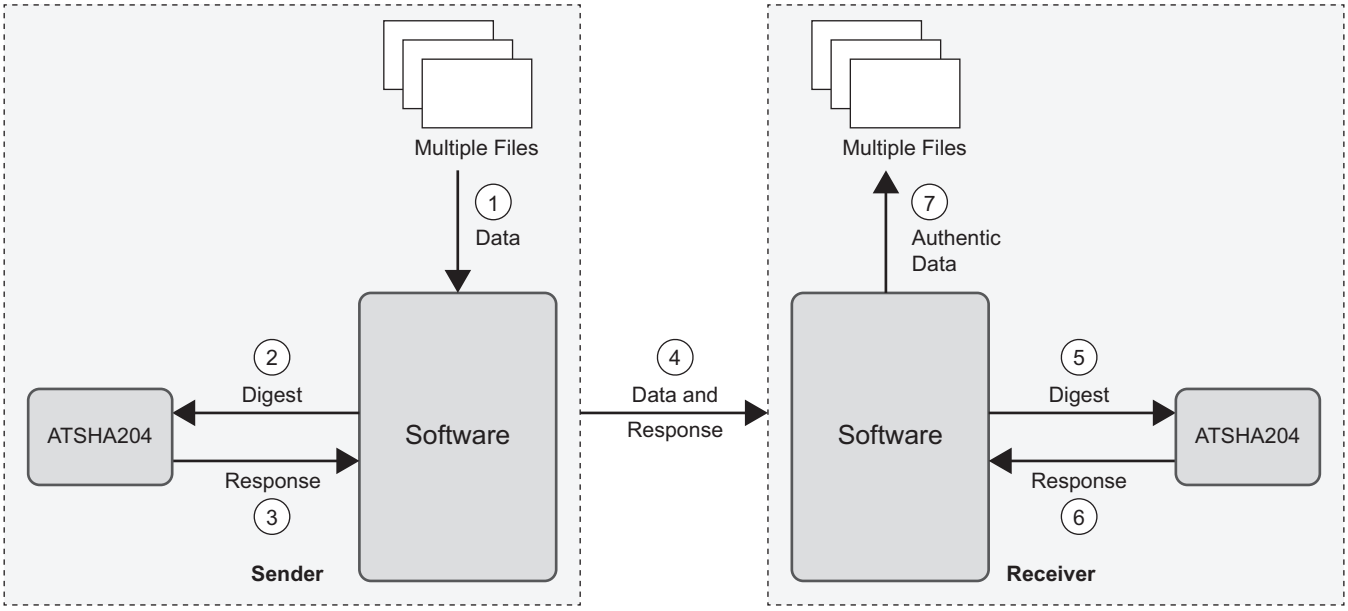


An additional level of security can be added for the data being transferred, i.e. encrypt the data or just verify the data integrity. The encryption process can be applied exactly like the data encryption scheme shown above.

The integrity of the data being exchanged can also be verified. Before sending the data, the sender calculates the data digest using SHA-256 algorithm. Then, ATSHA204 calculates the response by using the data digest as the challenge. The calculated response is sent alongside with the data to the receiver side. Upon receive, the receiver calculates the data digest, and the response then compares the received response with the calculated response. If the responses match, it means that the data has not been tampered by any attacker.

Figure 6-2 illustrates a configuration that utilizes two ATSHA204 devices in a radio network.

Figure 6-2. Data Integrity Verification



This configuration can be applied to these applications:

- Wireless node authentication
- Data over power lines authentication

7. Rolling Keys

In some applications, using the same key over and over can be a security risk. For instance, garage door openers. The ATSHA204 provides a feature for rolling keys. Normally, after a certain number of uses (perhaps as few as one), the current key value is replaced with the SHA-256 digest of its current value combined with some offset. The offset can be a constant, something related to the current system, or a random number.

One use for this capability is to permanently remove the original key from the device; replacing it with a key that is only useful in a particular environment. After the key is rolled, there is no possible way to retrieve the old value, which improves the security of the system.

There are two types of rolling key process:

- **Rolled Keys** — Uses the value of the current key to generate a new key, the generated key is called Rolled Keys.
- **Created Keys** — Uses the value of a parent key to generate a new key, the generated key is called Created Keys.

This operation can only be performed in a slot that permits the DeriveKey command. Proper configuration should be set on the chosen slot. To perform the operation, Nonce must be executed first to fill the TempKey value, and then DeriveKey command is executed by targeting the chosen slot. After the command execution, the target slot value will be updated with the digest generated from DeriveKey command.

8. Summary

The multipurpose functionality of the ATSHA204 CryptoAuthentication device makes them an exceptional tool for enabling hardware security. Nearly any application that requires authentication or individual identification of nodes can use ATSHA204 as part of its security solution architecture. If your security requirements vary from those listed in this document, or you are not sure that the ATSHA204 CryptoAuthentication devices fit your specific application, please contact your local Atmel representative. Chances are, Atmel has a product that will fit your needs.

Appendix A. Supporting Documents

- CryptoAuthentication product uses for the Atmel AT88SA10HS and the Atmel AT88SA102S. Please visit, http://www.atmel.com/Images/doc8663.pdf.

Appendix B. Revision History

Doc. Rev.	Date	Comments
8794A	12/2012	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