APPLICATION NOTE

Secure Personalization with Transport Key Authentication

ATSHA204A, ATECC108A, and ATECC508A

Introduction

The Atmel® CryptoAuthentication™ ATSHA204A, ATECC108A, and ATECC508A devices (crypto device) are state of the art Security IC hardware that has been developed for secure key storage. Often times, the end product that these devices are being used in are assembled and configured at third party test houses. For security reasons, one may not want to give the third party test houses secrets in the clear. The devices have the ability to securely transport these secrets to the subcontractor encrypted. Then internally to the device, it will decrypt the data and then program the information into the proper slots without being exposed to the outside.

Overview

The transport key allows for secure programming of the crypto devices without the third party programming company having access to the value of the Data zone. The programming company will be able to program and verify the content of these devices without having knowledge of the content.

The crypto devices have three different zones that can be programmed:

- Configuration Zone
- OTP Zone
- Data Zone

There are also two lock bits:

- One for the Configuration Zone
- One for both the Data and OTP Zones

The Configuration zone is always readable in the clear and once locked, is read-only. The Data and OTP zones are not writeable until after the Configuration zone is locked.

1 Acquiring a Transport Key

To obtain a transport key, contact Atmel at cryptosecrets@atmel.com.

As part of the request, it is required to provide:

- A Public Encryption Key – to ensure that you and only you know the value of the transport key.

In response, the following is sent from Atmel:

- Encrypted Transport Key
- Transport Keys ID – the crypto device is used to select the correct internal Transport Key when programming.

2 Zones

2.1 Configuration Zone

The Configuration zone is always readable in the clear; therefore, there is no reason for using a transport key to program the crypto device's Configuration zone. The Configuration zone should be locked using a validation CRC in the Lock command. The content of the locked Configuration zone should be mixed into the encryption key, along with the transport key when programming the Data zone. This ensures the device was configured as expected in order to program the correct Data zone values.

2.2 Data Zone

The Data zone is the secure area of the device. Use of a transport key is recommended to ensure no one has gotten access to the internal data of that device. The transport key is used as the initial secret that only the customer and the device know when issuing an encrypted write command to the Data zone. The key steps in securing the secrets are to:

1. Generate a random number and mix in the configuration making the configuration part of the SHA calculation.
2. SHA in the current value of the slot that will be used for the session key.
3. SHA in the unique transport key.

   As an option, mix in other non-secret OTP data to ensure proper programming of the OTP zone. The value should then be written back to the session slot.

4. Using the newly created session key, issue encrypted writes to each Data zone slot with the session key slot being the last slot programmed.

Once the device is programmed the Data and OTP zones should be locked.

2.3 OTP Zone

The OTP zone is always readable in the clear and therefore cannot contain secure information. In order to guarantee the value of the OTP zone:

1. Program the OTP zone.
2. Lock the OTP zone prior to encrypting the write to the Data zone.
3. The OTP zone content should then be mixed into the encryption key used for the Data zone.

2.4 Configuration

Use of a transport key only requires the Configuration zone to be locked prior to programming the Data zone. Until the Data zone is locked, the slot configuration information is not used, and no reads from the Data zone are allowed. Once the Configuration zone is locked, the Data zone becomes writable, and the encrypted data can be loaded into the crypto device with an internal transport key used for decryption.

3 Programming Flow

To setup the Session Key for programming the Data zone, the following commands are used:

Table 3-1. Program and Lock the Configuration Zone Commands

Command	Description
Nonce (Seed)	Load TempKey with the random number used during encryption.
GenDig (Config Zone 1)	Mix in the valid Configuration zone. This is recommended to ensure proper configuration of the slot security settings.
GenDig (OTP Zone 0)	Verify the OTP zone is programmed correctly. (Optional)
GenDig (OTP Zone 1)	Verify the OTP zone is programmed correctly. (Optional)
GenDig (Transport Key)	Add the transport key into the session key.
GenDig (Data Zone Slot Session)	Mix in the current value of the data slot.
Write (Data Zone Slot Session)	Store the session key to a slot.

Table 3-2. Write Commands

Commands	Description
Nonce (Seed)	
GenDig (Data Zone Slot Session)	Mix in the Session Key
Write (Data Zone Slot N)	Store the encrypted data into a slot

The slot used for the session key should be the last slot to be programming when writing the encrypted data to the device.

4 Revision History

Doc Rev.	Date	Comments
8860A	11/2015	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**