Shields UP: Counterfeit Protection of Disposable Applications with the ATSHA206A CryptoAuthentication™ Secure Element

Presenter: MH Eum – Senior Embedded Solutions Engineer, South Korea

Date: October 26, 2021

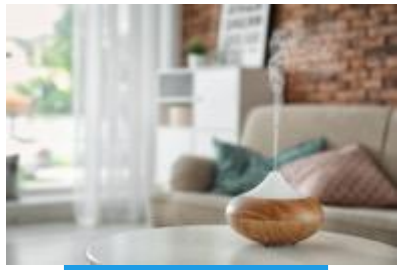
MICROCHIP

Disposable / Consumable

Application Examples

Insulin Pen

Handheld Hair Color Spray



Air Freshener Dispenser

Medical ECG

Printer Cartridge

CPAP Machine (Filter)

Electrode Pads

Skincare Brush

Save Costs, Reduce Risk, Increase Revenue

Brand protection and preserve quality

- Avoid counterfeit
- Avoid lower quality and lower performances
- Controlled ecosystem strategy

Save Costs, Reduce Risk, Increase Revenue

Revenue stream protection

- Start with authentication from the start
- Protect user experience
- Avoid discounted copies

Save Costs, Reduce Risk, Increase Revenue

Enable service revenue streams

- Maintenance service strategy
- Part replacement

Save Costs, Reduce Risk, Increase Revenue

Low integration cost with optimum form factor

- Reduce BOM by eliminating the PCB and diode
- Cost reduction with cheaper mechanical integration

What do those Systems Have in Common?

A Key: Protect it in a Microchip secure element

CryptoAuthentication™ Device Portfolio

ATECC608A

Typical Use Cases:

- Cloud authentication, firmware validation, accessory authentication, Intellectual Property (IP) protection, message encryption
- Asymmetric and/or symmetric key authentication model

ATSHA204A

Typical Use Cases:

- Firmware IP protection, accessory authentication, disposable and consumable applications
- Symmetric key authentication model
- Eliminating the cost of a PCB in disposable appliations (only when using 3-pin option)

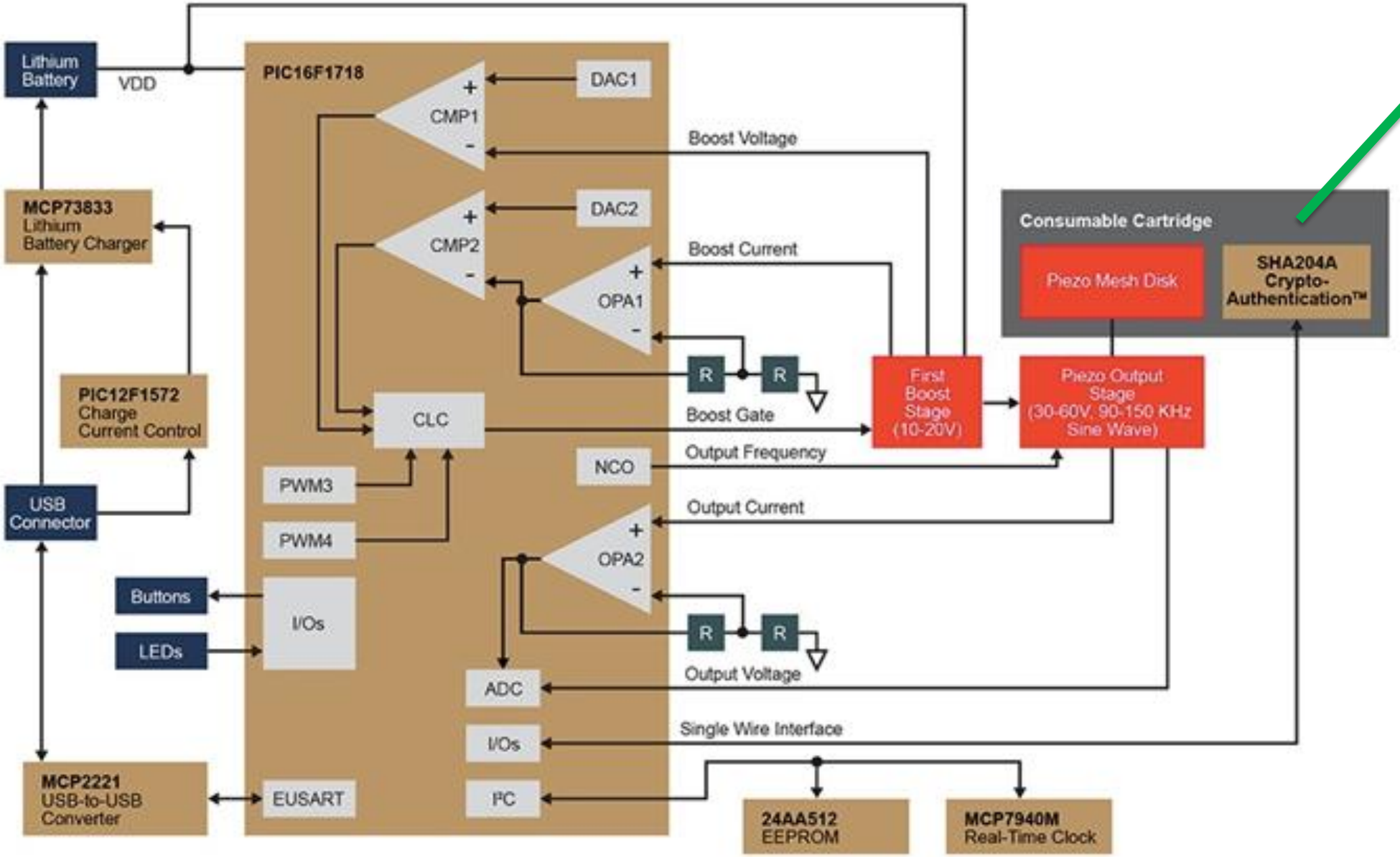
ATSHA206A 2-Pin Package

Typical Use Cases:

- Cartridge authentication to protect against cloning of consumable or disposable goods for consumer, cosmetic, industrial and medical applications
- Symmetric key authentication model
- Eliminating the cost of a PCB inside disposable applications

MICROCHIP

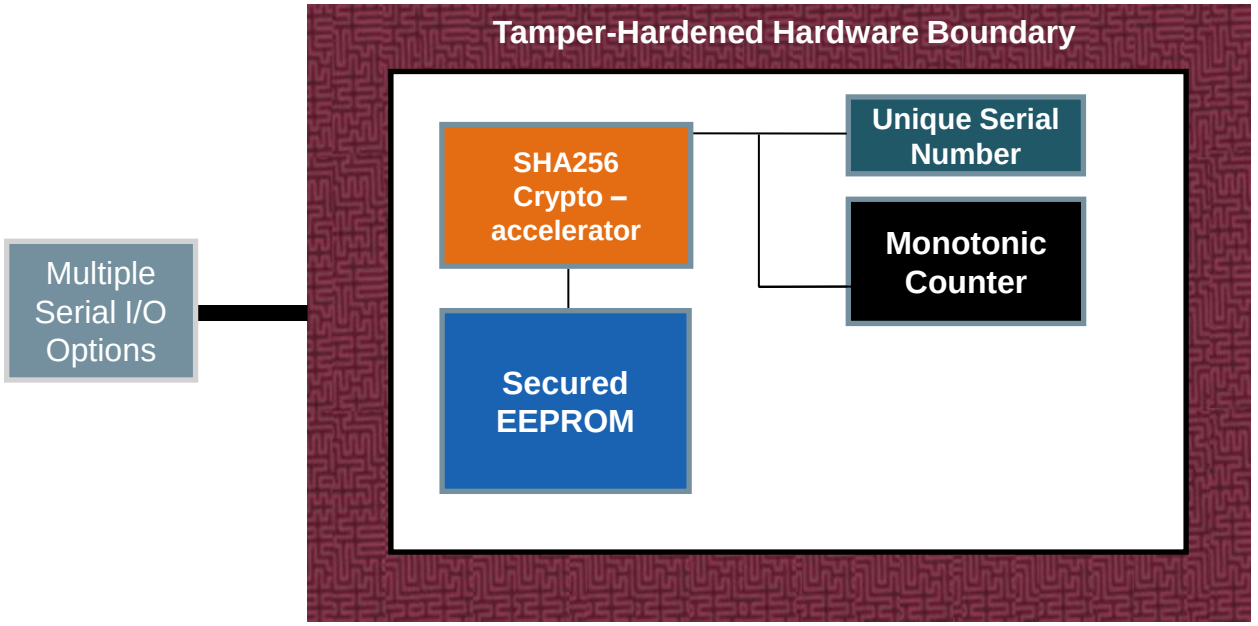
Reference Design: Nebulizer



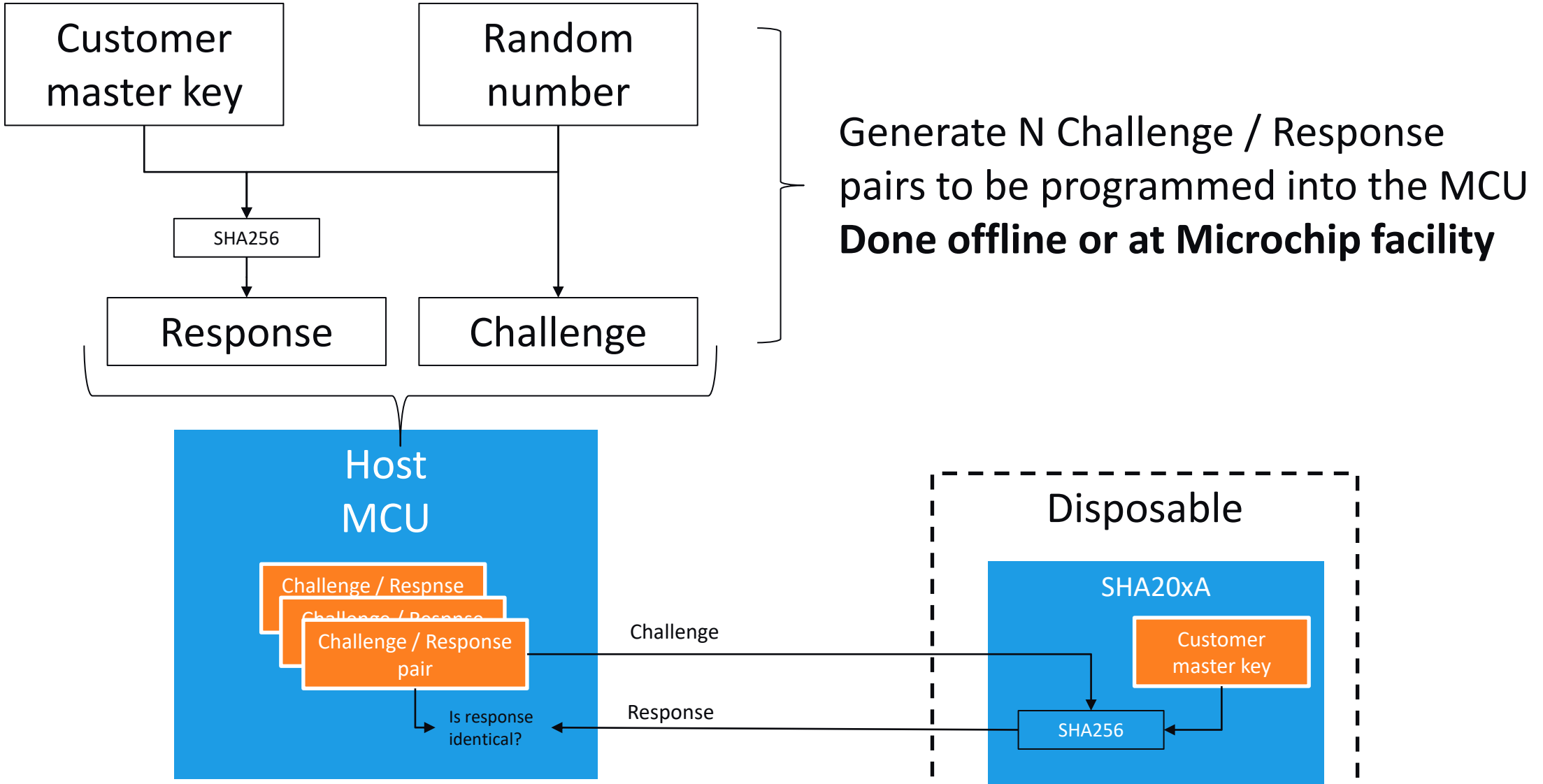
microchip.com/Medical

MICROCHIP

SHA206 Basic Architecture



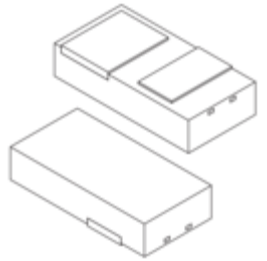
Transaction Diagram Example



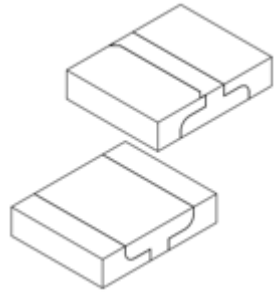
Alternatively an ATSHA204A could be used in the host to protect the symmetric key instead of pre-programming C/R

ATSHA206A Overview

- SHA-256 hash algorithm with 256-bit keys
- 248-byte EEPROM for configuration, keys and data:
  - Data zone: 5 slots of 32 bytes each
  - Configuration zone: 88 bytes for counting, locks and serial number
- Single-wire interface with parasitic power
- 2.5V to 4.5V supply voltage range
- <150 nA max sleep current
- Unique packaging solutions:
  - 2-Pad VSFN
  - 2-lead Top-Side-Bottom (TSB)



VSFN



TSB

ATSHA206A Device

Features

- **Parasitically-powered device with Single Wire Interface (SWI)**
  - Compatible with other CryptoAuthentication devices
  - No external cap required
- **Shorter set of commands versus the ATSHA204A**
  - DeriveKey, DevRev, MAC, Read, Write (with lock)
- **Configuration fixed**
  - 5 – dedicated slots
    - 1 – Symmetric secret (parent key)
    - 1 – Derived key
    - 3 – Data slots (1 always read/writable, 2 lockable)
- **Limited counter to 1024 uses**
  - Can be set during provisioning for a lower value
  - DeriveKey must be run after every 8 authentications (Key updating is optional based on DeriveKey mode)
- **CryptoAuthLib support**

ATSHA206A Device

Features

- **Parent Key**
  - Fixed value for a given customer / customer applications
  - Programmed during provisioning
  - Diversified keys can be supported
- **Derived Key**
  - Dedicated slot for deriving a key from the Parent key
  - Derived key is written during provisioning
- **Data Slots**
  - Three general purpose data slots for storing information
  - Two of these slots can be locked from further updates with Write Command

ATSHA206A Device

Packages / Prototype Units

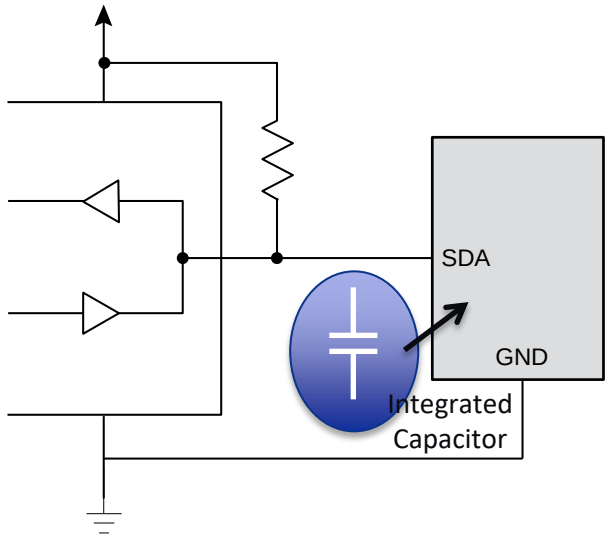
- **Prototype Units**
  - Are preconfigured units like the one on the ATSHA206A Trust Board
  - Available in 8-Pin UDFN (for proto only), 2-Pin VSFN(MBH) , 2-Pin TSB(MGH) packages
  - WLCSP can be supported

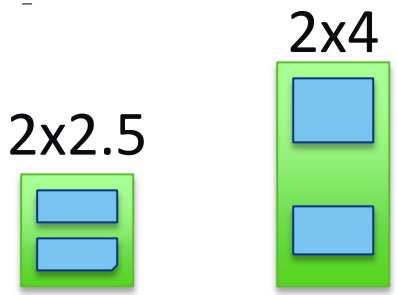
- **Production Units**
  - Configured based on customer information
  - Available in 2-Pin VSFN(MBH), 2-Pin TSB(MGH) packages
  - UDFN Not supported for Production

- **Generic blank devices not available**

From 3-Pin to 2-Pin Authentication

Let's Talk about Parasitic Power





- **Communications** take place over the **SDA** pin
- **Power from the SDA** pin when it is high and store it on the internal bypass capacitor.
- The resistor should be **pulling the SDA line high *only* during transmission of data**

Mechanical Considerations

With Disposables

- In **space-constrained** applications, (i.e. medical tubes) it is especially challenging to find a small enough form factor to achieve secure authentication
- Can the disposable accommodate a PCB or avoid it ?
- Paradoxically, **smaller is not always better** … because of contact size from a large size host unit, often driven by standardization or environmental conditions, the application requires contact solutions
- Current contact packages in the market **only** have pads **available on one side (bottom)** of the package

Package Solutions

- **ATSHA204A**
  - UDFN8, SOIC8, TSSOP8, SOT323, 3-Pin-RBH contact

- **ATECC608**
  - UDFN8, SOIC8, WLCSP(contact BU)

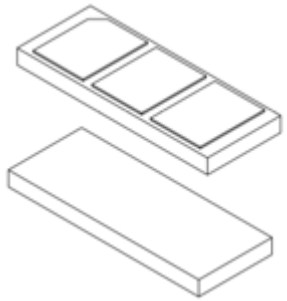
- **ATSHA206A**
  - Target primary packages 2-pins 2x4 and 2x2.5

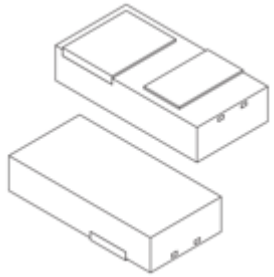
Package Size Matters

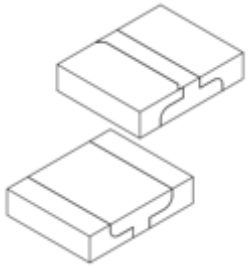
How to reduce cost and simplify the overall system design …

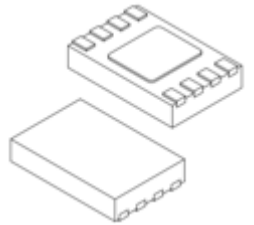
… ELIMINATE the PCB

Mechanical Solutions









Device	ATSHA204A	ATSHA206A	ATSHA206A	ATSHA204A ATECC608
Package	RBH	VSFN	TSB	uDFN8
Pin Count	3	2	2	8
Parasitic Power	No	Yes	Yes	No
Size(mm)	2.5x6.5	2x4	2x2.5	2x3
PCB needed	No	No	No	Yes

The Mechanical Solutions

TSB Package 2x2.5mm

Clipping

Side Contacts

Best suited for 2x2.5mm

Side and bottom

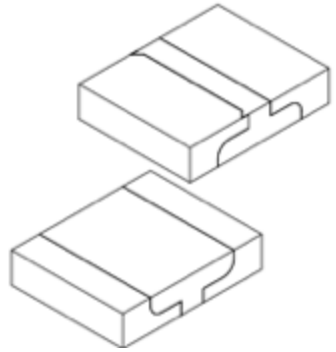
Sit "In"

Press Fit

Pogo pin Bottom

Pogo pin Above

= Metal Contact



System Implementation Variations

For Accessories and Disposables

Microcontroller		ATSHA204/206 disposables
• Root Shared key • Challenge/response pair unique for each host • Possibility of cloning the host (micro)	Symmetric	• Personalized secret • Secret key same in every client • no PCB

Microcontroller	ATSHA204		ATSHA204A disposables
• No secret in the Micro • Cannot share host & client bus (dedicated)	• Shared key (root) • Random challenge from SHA204 • Leverage diversified key for disposable authentication	Symmetric	• Diversified key in client • Each client is unique (blacklist) • no PCB (RBH)

Microcontroller	ATECC608		ATSHA204 disposables
• No secret in the Micro • Cannot share host & client bus (dedicated)	• Shared key (root) • Random challenge from ECC608 • Diversified key for disposable • PKI to Cloud	Symmetric	• Personalized Secret • Secret key different in every client • Require PCB (uDFN)

System Implementation Variations

For Accessories and Disposables

Microcontroller		ATECC608 disposables/accessories
• Public key to verify signature (or verified by Cloud) • No secret in the micro • Hard to clone the host (micro) • MCU need to have ECDSA verify	Asymmetric	• Personalized secret • Secret key different in every client • Require PCB

Microcontroller	ATECC608		ATECC608 disposables/accessories
• No secret in the Micro • Cannot share host & client bus (dedicated)	• Use PKI for Cloud authentication • Compute ECDSA verify with Disposable	Asymmetric	• Personalized secret • Secret key different in every client • Require PCB

Question Guide

PCB or no PCB?

- **Is there a PCB on your disposable**
  - Yes – look at ATECC608 or ATSHA204A uDFN8 or SOIC8
  - No – no PCB allowed in the cartridge, go to next question

- **Mechanical constraints (2-pin vs 3-pin)**
  - 3-pins :
    - Is a 6.5 x 2.4mm module size OK? → SHA204A RBH
      - Need for large pads for contact due to physical tolerance
    - Can the system tolerance 3-pin (Vcc, I/O, GND) No? Look at the 2-pin options
  - 2-pins :
    - Is 2x2.5mm device size OK? → SHA206A TSB
      - Smallest form factor in 2-pin
    - Is 2x4mm device size preferred? → SHA206A VSFN
      - Larger 2-pin form factor helps with physical tolerance

24

Mechanical Skillsets

A Partner Solution

- **How to address the cartridge assembly questions?**
- **The production questions: part orientation, handling, glue?**

Our partners play an important role:

- **Garrett Technology**
  - Design house – electronics + mechanical expertise
- **Optimal Design**
  - Design house – electronics + mechanical expertise
- **Jabil**
  - Contract manufacturer + design services
- **Lindal**
  - Mechanical Engineering

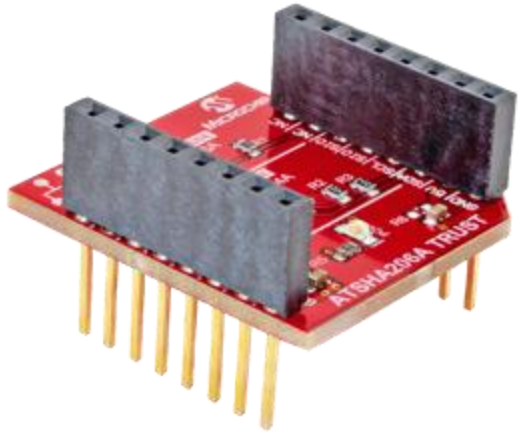
You want to join ? Apply to the Microchip Design Partner program

ATSHA206A Trust Board

How to Get Started

ATSHA206A Trust Board

Features



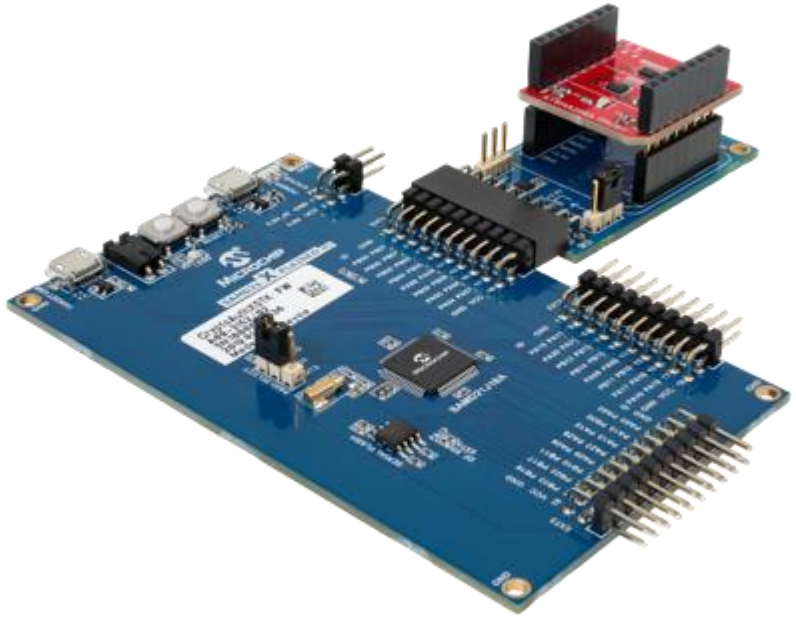
- **1 – ATSHA206A Prototype Unit (UDFN)**
  - Preconfigured and locked with prototype secret
  - Capable of 1024 Uses
  - Can write and lock data slots
- **1 – ATSHA204A Host unit (UDFN)**
  - Preconfigured and locked with ATSHA206A prototype secret
  - Can be used to derive new keys in sync with ATSHA206A
- **Implemented as a MikroBus™ extension board**
  - ATSHA206A Connected to serial port signals
  - ATSHA204A Connected to I^2C signals

ATSHA206A Trust Board

Software Updates

- **DM320118 – Trust Platform**
  - Firmware update will be posted on the DM320118 Webpage
  - Kit Protocol modifications allows for proper identification of ATSHA206A via CryptoAuthLib

- **DM320109 – CryptoAuth-XSTK**
  - Firmware update will be posted on the DM320109 Webpage
  - Kit Protocol modifications allows for proper identification of ATSHA206A via CryptoAuthLib



ATSHA206A Trust Board

Firmware

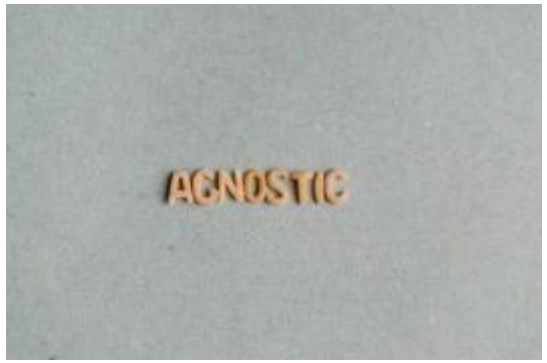
- **Use Cases / Firmware**
  - Latest Release of **Cryptoauthlib** has support for SHA206A (C version only no python support)
  - No Trust Platform use case at present time (Oct'20)
  - Two Code Examples available:
    - Packet Based Authentication
    - Disposable Authentication

Takeaways

Easier onboarding with
predefined use cases

Quick development with
simple toolsets

Simpler flows leveraging
Microchip Secure Provisioning Service



Architecture agnostic with any controller

Join us for our upcoming session
Accessories Authentication with Secure Elements
Tuesday, November 23rd, 10:30-11:30am

MICROCHIP