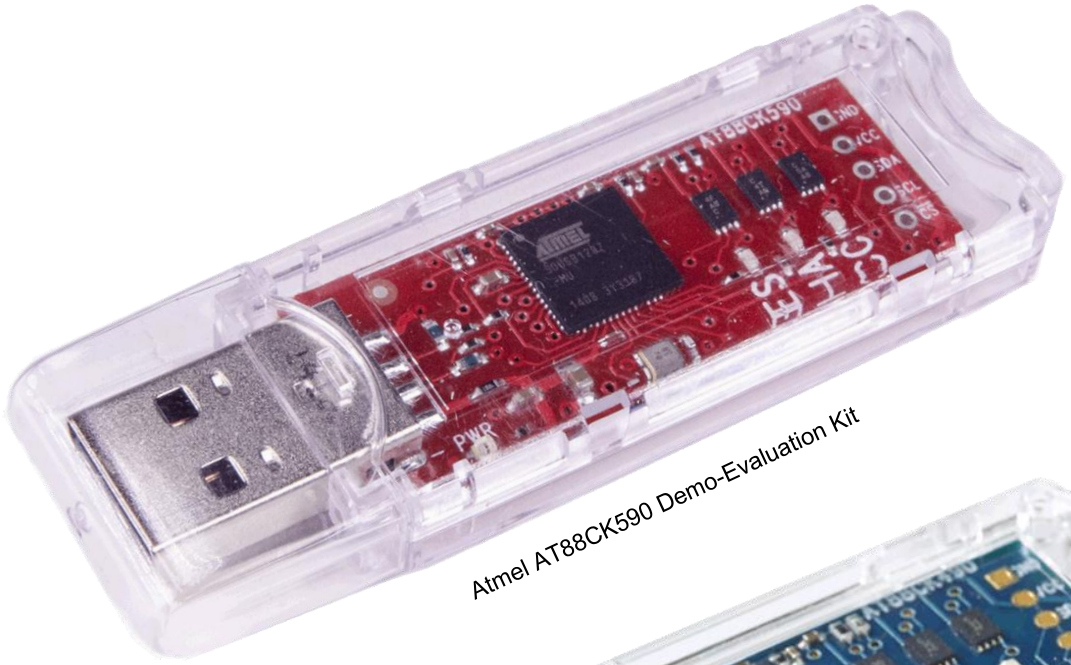
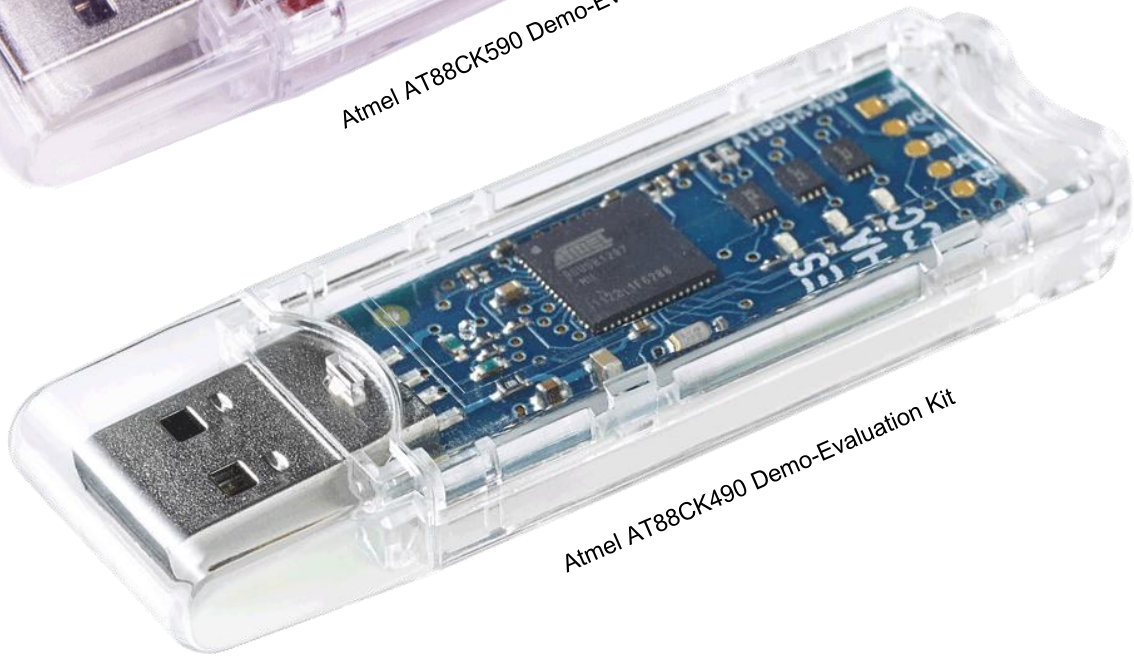
# AT88CK490 and AT88CK590

## Atmel® CryptoAuthentication™ USB Dongle Demo-Evaluation Kits For ATSHA204A, ATAES132A, ATECC108A, and ATECC508A

**HARDWARE USER GUIDE**




Atmel AT88CK590 Demo-Evaluation Kit



Atmel AT88CK490 Demo-Evaluation Kit

**Atmel CryptoAuthentication USB Dongle Demo-Evaluation Kits**

## Introduction

The Atmel® CryptoAuthentication™ USB Dongle Evaluation Kits are the ideal way to evaluate the performance and applicability of the Atmel Family of CryptoAuthentication devices. Each kit contains three devices:

- **AT88CK490 Kit** (Blue PCB): ATAES132A, ATSHA204A, and ATECC108A
- **AT88CK590 Kit** (Red PCB): ATAES132A, ATSHA204A, and ATECC508A.

The kits are USB dongles that allows the interested evaluator to plug it into a PC and use the evaluation and development software package called Atmel CryptoAuthentication Evaluation Studio (“ACES”) that is easily downloadable from the Atmel website.

Each kit includes an Atmel AT90USB1287 AVR® microcontroller which provides a convenient USB 2.0 Full Speed interface allowing users to understand and experiment with the CryptoAuthentication devices. Developers can use the provided 5-pin interface at the end of the board and can be used to monitor the $I^2C$ protocol. Atmel also offers a socketed board called the Atmel AT88CK101 for the purpose of firmware development, which allows the user to try differently configured devices on a target system. Typically, users will start with one of the USB Dongle kits for evaluation and part selection and then migrate to the AT88CK101 for the purpose of development. Both kits run the ACES configuration environment software package, which provides continuity from the evaluation to development stage.

Complete support for this kit is available at www.atmel.com/cryptokits.

## Kit Contents

- CryptoAuthentication USB Dongle Evaluation Kit

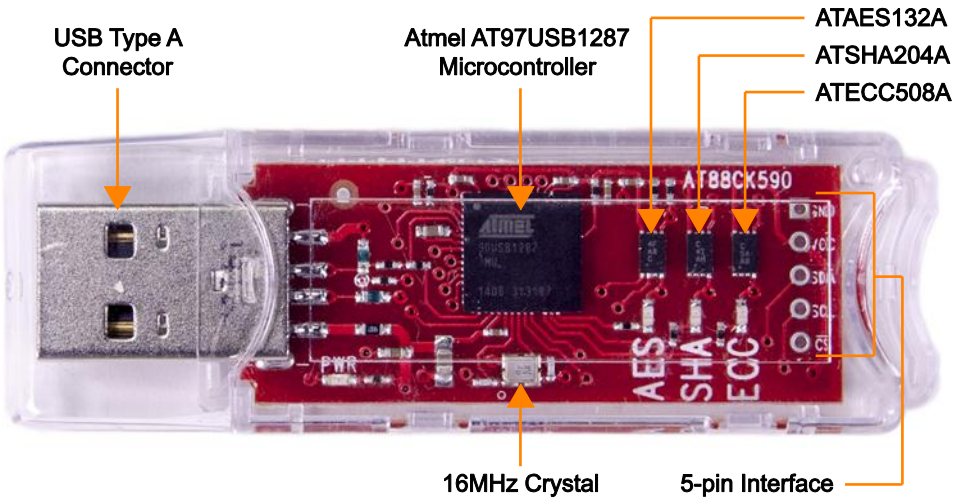
## CryptoAuthentication USB Dongle Kit Features

- Atmel ATAES132A CryptoAuthentication IC: $I^2C$ Address (`0xA0`)
- Atmel ATSHA204A CryptoAuthentication IC: $I^2C$ Address (`0xC8`)
- Atmel ATECC108A CryptoAuthentication IC: $I^2C$ Address (`0xC0`) – AT88CK490 *Only*
- Atmel ATECC508A CryptoAuthentication IC: $I^2C$ Address (`0xC0`) – AT88CK590 *Only*
- Atmel AT90USB1287AVR
  - 128KB of In-system Programmable Flash
  - 4KB EEPROM
  - 8KB Internal SRAM
- USB 2.0 Full Speed Device
- Power LED (Red)
- Three Status LEDs (Blue)

## Table of Contents

## Board Overview

**Figure 1. Top Side Placement of Components** (AT88CK590 Shown)

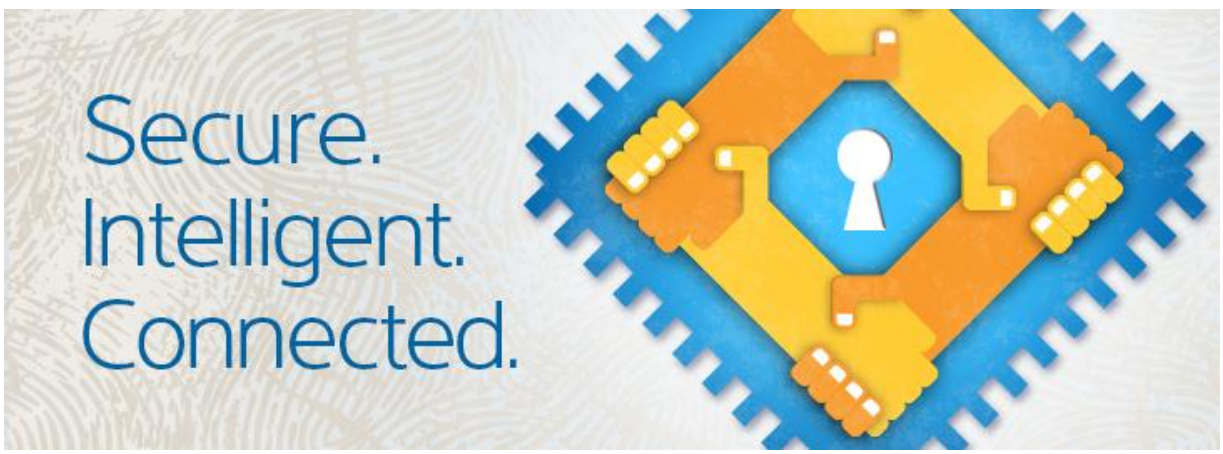



## CryptoAuthentication Device Family Overview

Atmel offers the industry's widest portfolio of crypto elements with ultra-secure hardware-based key storage to provide confidentiality, integrity, and authentication. The Atmel crypto element devices included in each kit are noted below:

**Table 1. Atmel Crypto Element Devices**

| Demo-Evaluation Kit | ATAES132A | ATSHA204A | ATECC108A | ATECC508A |
|---|---|---|---|---|
| AT88CK490 | ● | ● | ● | |
| AT88CK590 | ● | ● | | ● |



## ATAES132A

The ATAES132A with hardware-based key storage is a very fast, high-security, Serial 32Kb EEPROM that enables authentication and confidential nonvolatile data storage. It is a direct drop-in for industry standard Serial EEPROMS and implements Advanced Encryption Standard (AES) cryptography. Access restrictions for the 16 user zones are independently configured and any key can be used with any zone. Keys can also be used for standalone authentication. The AES-128 crypto engine operates in AES-CCM mode to provide authentication, stored data encryption/decryption, and Message Authentication Codes (MACs). Data encryption/decryption can be performed for internally stored data or for small external data packets depending upon the configuration. Data encrypted by one ATAES132A device can be decrypted by another, and vice versa. The User Memory can be accessed directly with standard SPI or $I^2C$ commands. The device's secure Serial EEPROM architecture and packages are compatible with standard SPI and $I^2C$ EEPROM footprints. This allows insertion into many existing Serial EEPROM applications.

For additional information please go to: www.atmel.com/devices/ATAES132A.aspx

## ATSHA204A

The cost-effective ATSHA204A with hardware-based key storage provides flexible user-configured security to enable a wide range of applications. With cryptographic algorithms built-in, it is easy to design in without having cryptographic expertise. The ATSHA204A integrates the 256-bit Secure Hash Algorithm (SHA-256) and contains 4.5Kb EEPROM for secure key and data storage. Features such as small outline plastic package and either an $I^2C$ or a Single-Wire Interface (SWI) make the ATSHA204A ideal for handheld electronic systems or any space-constrained embedded system.

Implementing host-side security to provide a full symmetric authentication system solution is very easy. The ATSHA204A includes client and host security capabilities that offloads key storage and the execution algorithms from the microcontroller, which significantly reduces system cost and complexity.

For additional information please go to: www.atmel.com/devices/atsha204a.aspx.

## ATECC108A

The ATECC108A supports full 256-bit Elliptic Curve Cryptography (ECC) and has no need for secure storage in the host. The ATECC108A includes an EEPROM array for storage of up to 16 keys, miscellaneous read/write, read-only or secret data, consumption logging, and security configurations. Access to memory can be restricted in a variety of ways and the configuration can be locked to prevent changes.

The ATECC108A features defense mechanisms to prevent physical attacks on the device or logical attacks on the data transmitted between the device and the system. Hardware restrictions on the keys generation or use provide further defenses. Access to the device is made through a standard $I^2C$ Interface at speeds of up to 1Mb/s. It supports a SWI, which can reduce the number of GPIOs required on the system MCU. Multiple ATECC108A devices can share the same bus, which saves processor GPIO usage in systems with multiple clients.

For additional information please go to: www.atmel.com/devices/atecc108a.aspx.

### ATECC508A

The ATECC508A with secure hardware-based key storage supports full 256-bit ECC and is the first device to integrate ECDH (Elliptic Curve Diffie–Hellman) key agreement, which makes it easy to add confidentiality (encryption/decryption) to digital systems including Internet of Things (IoT) nodes used in home automation, industrial networking, accessory and consumable authentication, medical, mobile, and other applications.

In addition to ECDH, the ATECC508A has ECDSA (Elliptic Curve Digital Signature Algorithm) sign-verify capabilities built-in to provide highly secure asymmetric authentication. The combination of ECDH and ECDSA makes the device an ideal way to provide all three pillars of security (confidentiality, data integrity, and authentication) when used with MCU or MPUs running encryption/decryption algorithms (e.g. AES) in software. Similar to all Atmel CryptoAuthentication products, the ATECC508A employs ultra-secure hardware-based cryptographic key storage and cryptographic countermeasures which are more secure than software-based key storage.

Able to support asymmetric authentication, there is no need for secure storage in the host. An EEPROM array is included for storage of up to 16 keys, miscellaneous read/write, read-only or secret data, consumption logging, and security configurations. Access to memory can be restricted in a variety of ways and the configuration can be locked to prevent changes. Access is through a standard $I^2C$ Interface at speeds of up to 1Mb/s. It supports a SWI, which can reduce the number of GPIOs required on the system MCU. Multiple ATECC508A devices can share the same bus, which saves processor GPIO usage in systems with multiple clients.

The ATECC508A can generate high-quality FIPS random numbers for any purpose ensuring that replay attacks (i.e. re-transmitting a previously successful transaction) always fail. System integration is easy due to a wide supply voltage range (2.0V to 5.5V) and an ultra-low sleep current (<150nA).

For additional information please go to: www.atmel.com/devices/atecc508a.aspx.

## Get Started

The following discusses the steps to start using the demonstration-evaluation kit.

### Step 1 Download ACES Software at www.atmel.com

ACES is a Windows-based application software used to interface with the demo-evaluation kits. ACES works with the Kit Protocol noted in Step 5. The ACES software is located at:

www.atmel.com/tools/ATMELCRYPTOEVALUATIONSTUDIO_ACES.aspx

Register and download the ACES Setup File (ACES_Setup_x.x.x.exe). Install the setup file and follow the instructions in the set-up wizard to complete the installation. The ACES Configuration Environment (CE) icon will be placed on the desktop.

The AT88CK590 requires ACES 5.0.0 or later.

The AT88CK490 will work with earlier versions of ACES.

Start the ACES CE Software Program. Either open the program via the desktop icon or via the ***Start menu*** > ***All Programs*** > ***Atmel Crypto Solutions*** > ***ACES*** > ***ACES CE***.

When the kit is plugged into the USB port, ACES will automatically detect that the kit is attached and launch the ***Kit Detection*** dialogue box.

## Step 2 Power-Up the USB Dongle Kit

The kit is powered through a USB Port. Simply insert the board into an open USB port and then the following sequence will occur:

1. The red power LED will illuminate.
2. The device will go through a self-test.
3. All three blue LEDs will illuminate.

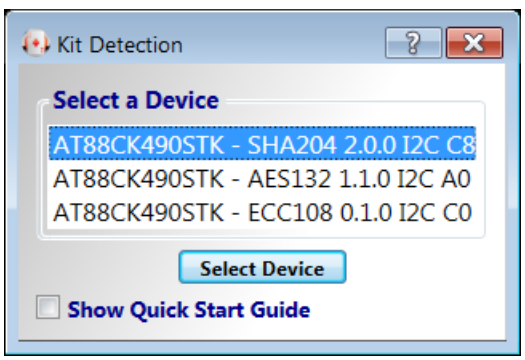
**Figure 2. Kit Powered Through USB Port**

## Step 3 Select the Atmel CryptoAuthentication Device to Evaluate

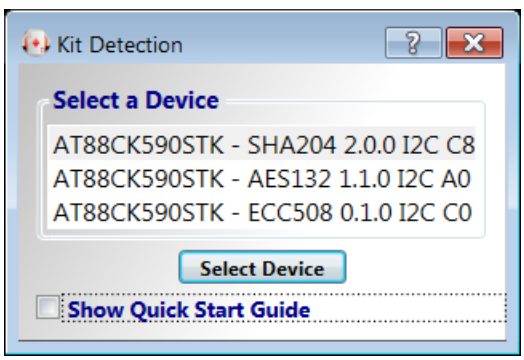
Choose which device to evaluate by using the ***Kit Detection*** dialogue box that will appear as shown below. Once the device is selected, the blue LED corresponding to that device will flash and the other device status LEDs will be disabled. (Please note that the LED will also flash when traffic is going to and from that device.) For additional information regarding the use of ACES and on the devices when first power-up, check the ***Show Quick Start Guide*** checkbox.

**Figure 3. Kit Detection Dialogue Box**

**AT88CK490 Dialogue Box**




**AT88CK590 Dialogue Box**



## Step 4 Use ACES to Evaluate the Device

Please refer to www.atmel.com/tools/ATMELCRYPTOEVALUATIONSTUDIO_ACES.aspx for detailed information about ACES. An example of the ACES configuration screen is shown below:

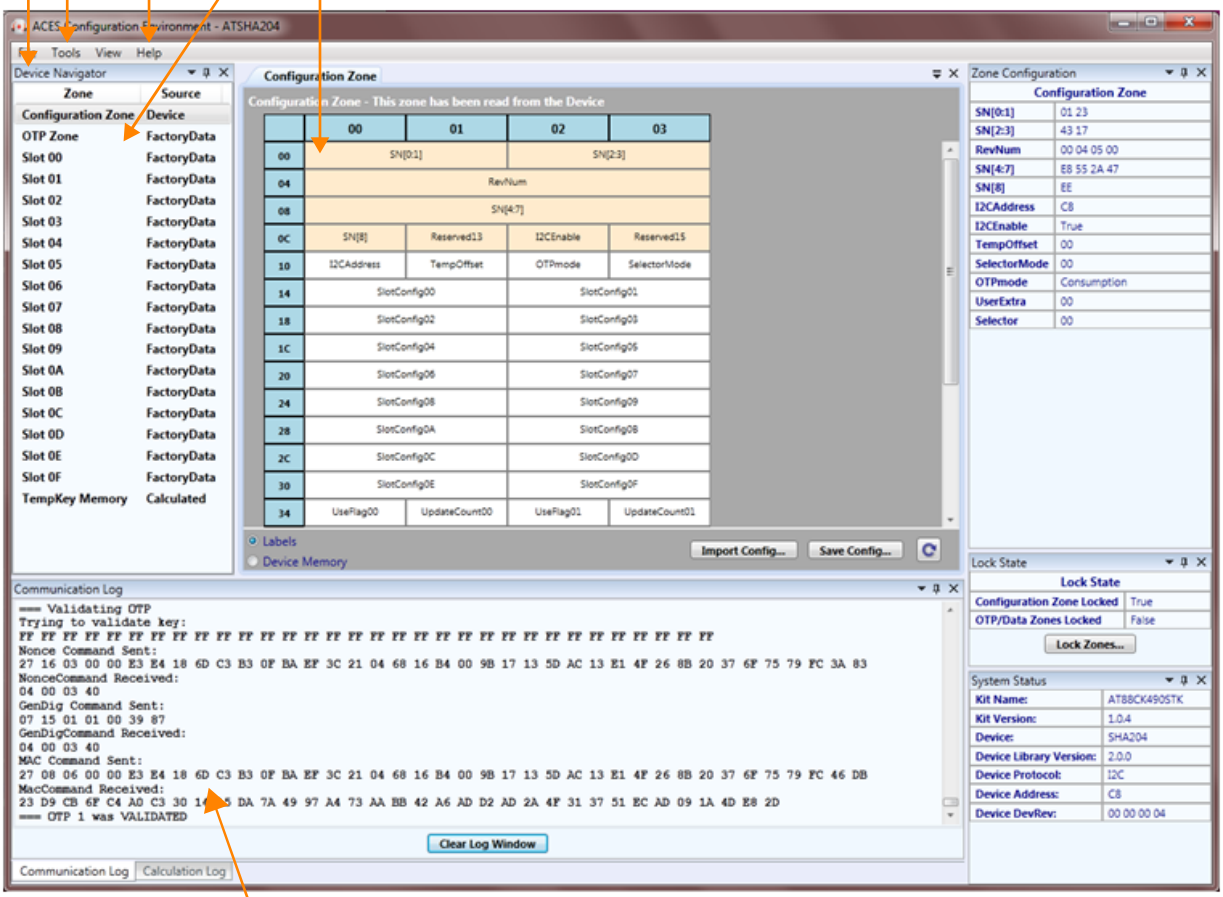
**Figure 4. ACES – Software Environment for Demo, Evaluation, and Design**

***Device Navigator*** Generates, Stores, and Reloads Configuration Files.

***Tools*** Demos and Wizards Commands

***Help*** Datasheet Explained via Help Screens

***Configuration Zone*** Displays EEPROM Registers and Contents.




***Communication Log***

- Teaches Command, Structure, and Encoding.
- Displays Actions and Results.

### Step 5 Optional: USB Dongle Kits Communication Protocol

It is possible to obtain access to the communication protocol of the CryptoAuthentication USB Dongle kits which are designed to interface with either a Microsoft HID driver or the Atmel AVR CDC driver. Both interfaces use the same Atmel CryptoAuthentication Kit Protocol, which is an ASCII-based interface to the AT90USB1287 AVR microcontroller located on the kit. The protocol allows control of all devices on the $I^2C$ bus. Source code for the kit protocol is available for download at: www.atmel.com/cryptokits.

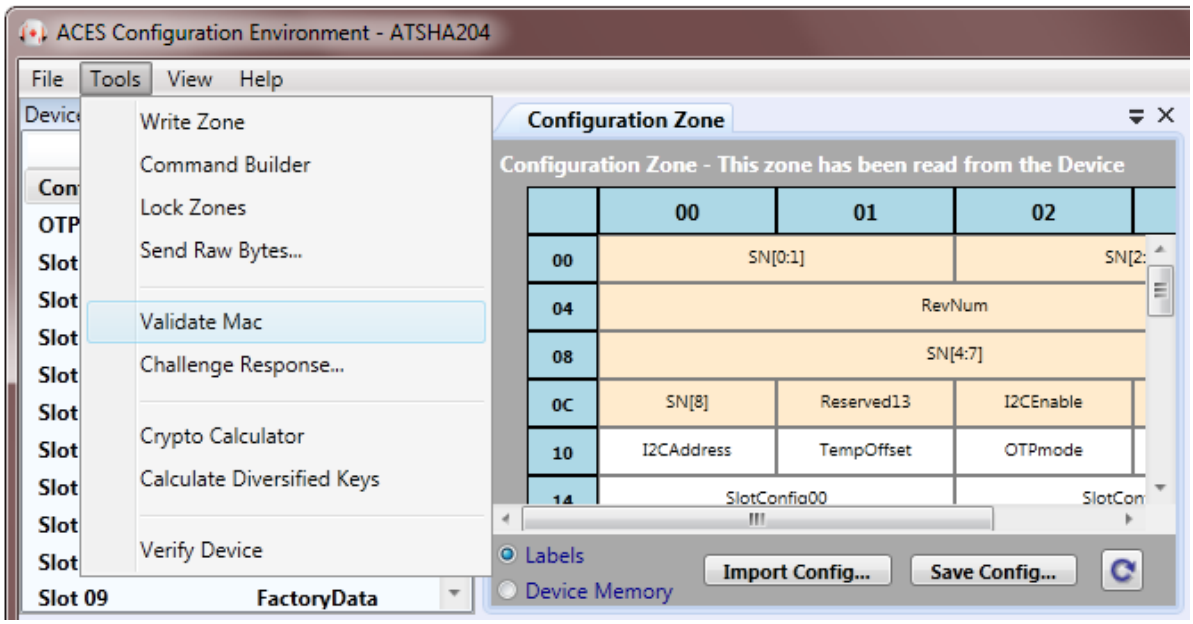
## ACES Evaluation Example – Validate MAC Command

### Step 1 Launch ACES and Select ATSHA204A

### Step 2 Launch the Validate Mac Window

On the main menu, select ***Tools*** > ***Validate MAC***.

**Figure 5. Validate MAC Tools Menu**



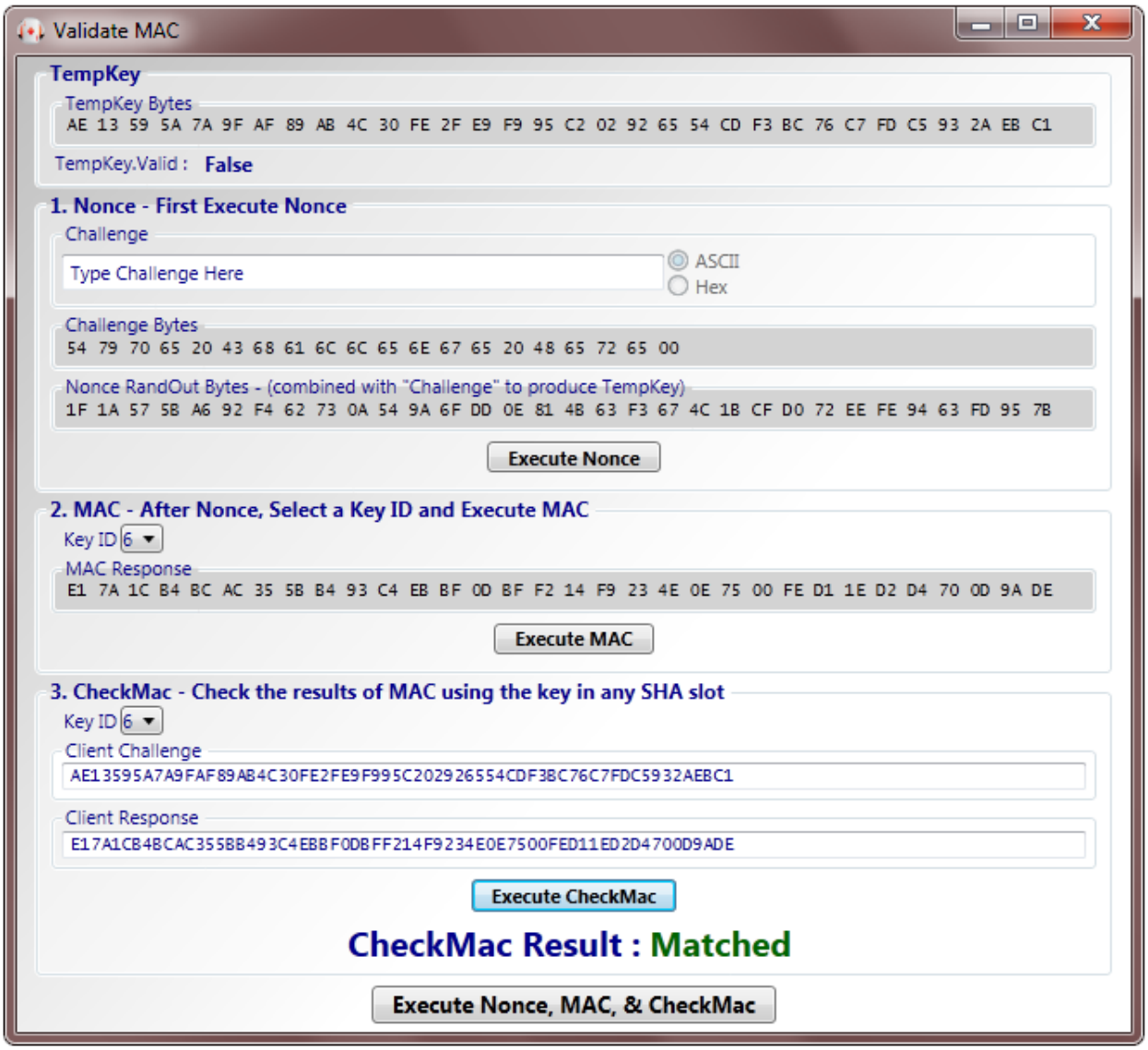
### Step 3 Execute the Validate Mac

The ***Validate MAC*** window should now be displayed.

1. Click on the ***Execute Nonce*** button.
2. Click on the ***Execute MAC*** button.
3. Click on the ***Execute CheckMac*** button.

The ***CheckMac Result*** line should indicate **Matched**. See Figure 6.

**Figure 6. Validate MAC Pane**




Congratulations, the Atmel USB Dongle Demonstration-Evaluation Kit is up and running. See ACES online help for additional information. Additional samples can be found at:
http://www.atmel.com/forms/Samples.asp?family_id=699

# Schematics

**Figure 7. Microcontroller and Status Circuitry Schematics**

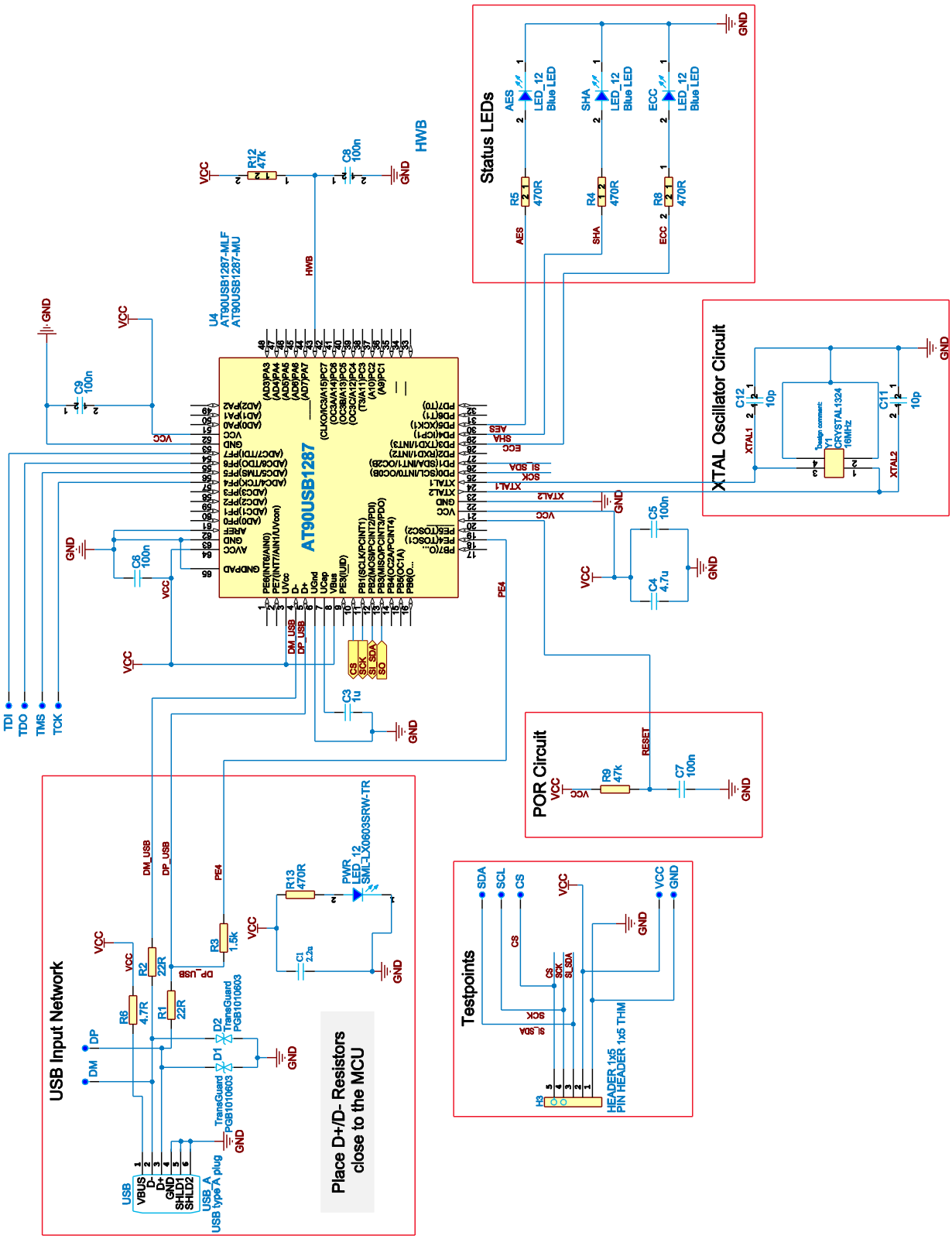
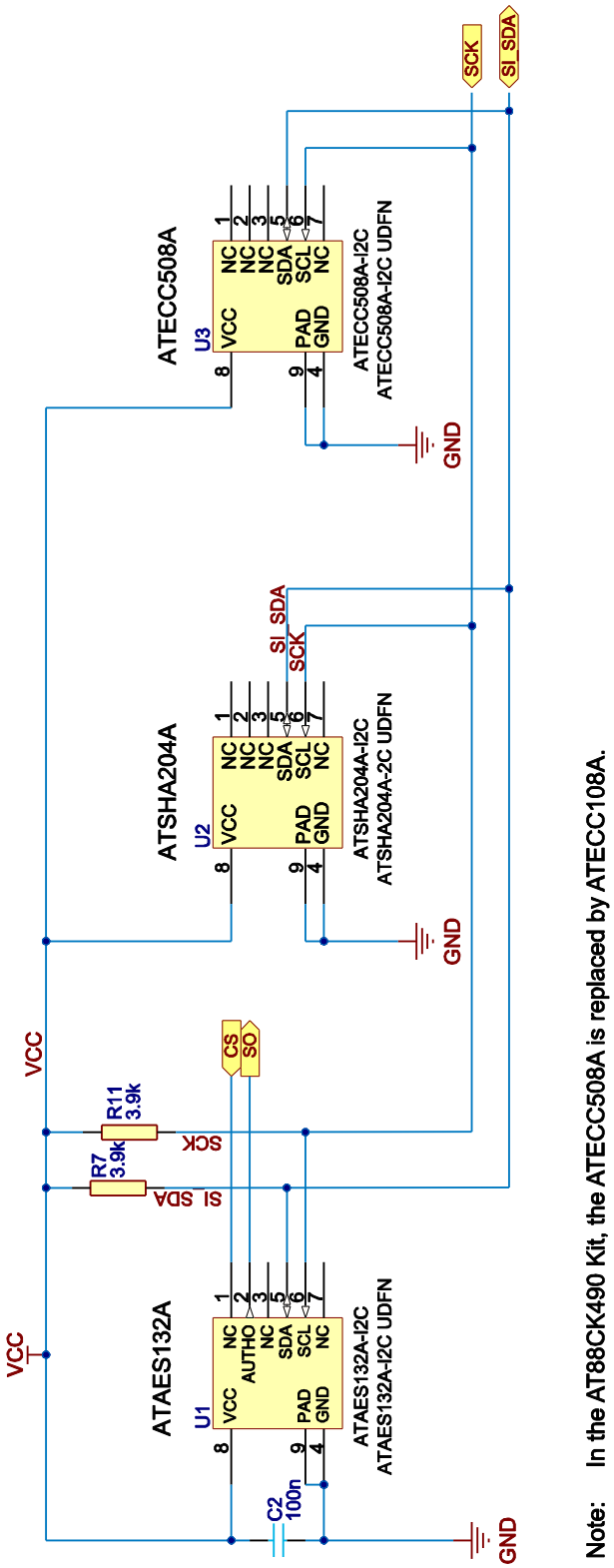


**Figure 8. Crypto Device Circuitry Schematics**



## Firmware Upgrade

For firmware upgrades, please refer to the application note, “Upgrading the Atmel CryptoAuthentication/Tempsensor Kit Firmware Using FLIP”, which is located at the following site:

http://www.atmel.com/tools/AT88CK590.aspx?tab=documents.

## References and Further Information

Schematics, Gerber files, Bill Of Materials (BOM), development, and demonstration software are conveniently downloadable from the Atmel website at www.atmel.com/cryptokits.

### Additional Evaluation Kits

Atmel offers a range of kits to support the Atmel CryptoAuthentication device development all the way to small-run production. The Atmel kits run ACES software to configure the CryptoAuthentication devices. The combination of the user friendly hardware and software presents users with exactly what is needed through the process.

For information on the latest and all of the available Atmel Crypto Kits please go to:
http://www.atmel.com/CryptoKits/CryptoAuthentication_SelectorGuide.pdf

#### Start with a Demo-Evaluation Kit

The AT88CK590 and AT88CK490 demo-evaluation kits includes three devices each. Once the user gets a feel for the operation and performance of the devices, the next task is development.


#### AT88CK101 or CryptoAuthXplained Development Kit

The AT88CK101 development kit is a socketed kit that allows the developer to program the Atmle CryptoAuthentication devices and then install those devices in their system. Versions that support the various device package types are available.

The CryptoAuthXplained and CryptoAuthXplained Pro *(Coming Soon)*, which are standard 10/20-pin daughterboards instantly adds the Atmel CryptoAuthentication devices to the Xplained or XplainedPro development environment boards.

#### AT88CK9000 Secure Personalization Kit Option

The Atmel AT88CK9000 secure personalization kit allows programming of small batches of ATSHA204A devices quickly, easily, and cost-effectively. This option decreases the cycle times of prototype, pre-production, and lower-volume production, improving time to market. The AT88CK9000 securely programs up to 5 or 10 devices simultaneously depending on the package option. Running production is as easy as pressing a *yellow* button...*literally*.

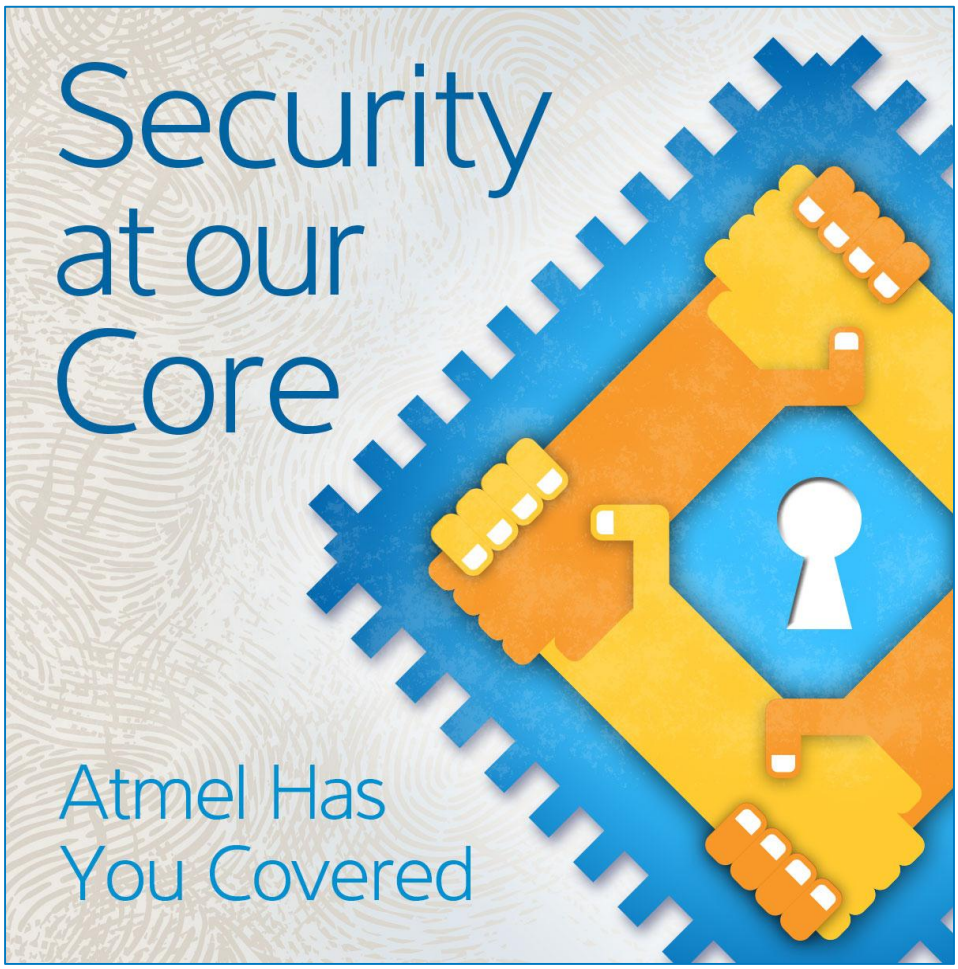
## ATMEL EVALUATION BOARD/KIT IMPORTANT NOTICE AND DISCLAIMER

This evaluation board/kit is intended for user's internal development and evaluation purposes only. It is not a finished product and may not comply with technical or legal requirements that are applicable to finished products, including, without limitation, directives or regulations relating to electromagnetic compatibility, recycling (WEE), FCC, CE or UL. Atmel is providing this evaluation board/kit “AS IS” without any warranties or indemnities. The user assumes all responsibility and liability for handling and use of the evaluation board/kit including, without limitation, the responsibility to take any and all appropriate precautions with regard to electrostatic discharge and other technical issues. User indemnifies Atmel from any claim arising from user's handling or use of this evaluation board/kit. Except for the limited purpose of internal development and evaluation as specified above, no license, express or implied, by estoppel or otherwise, to any Atmel intellectual property right is granted hereunder. ATMEL SHALL NOT BE LIABLE FOR ANY INDIRECT, SPECIAL, INCIDENTAL, OR CONSEQUENTIAL DAMGES RELATING TO USE OF THIS EVALUATION BOARD/KIT.

ATMEL CORPORATION
1600 Technology Drive
San Jose, CA 95110
USA

## Revision History

| Doc Rev. | Date | Comments |
|---|---|---|
| 8941A | 05/2015 | 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**

# Mouser Electronics

Authorized Distributor

Click to View Pricing, Inventory, Delivery & Lifecycle Information:

Microchip:
AT88CK590