Application Note

Atmel Crypto Evaluation Studio Overview

Features

- Configuration environment (CE) for the Atmel® ATSHA204 and the Atmel ATAES132 CryptoAuthentication™ device
- Atmel ATSHA204 device demonstration
  - Interactive challenge-response demo
- Complete help system
  - Context-sensitive Atmel Crypto Evaluation Studio (ACES) CE and demo help
  - Simple walkthrough help
  - Integrated ATSHA204 and ATAES132 datasheet help
  - Integrated application note help
- Supports the following development kits:
  - Atmel AT88CK101 kit
  - Atmel AT88CK454BLACK kit
  - Atmel AT88CK427GREEN
  - Atmel ATAVRSECURITYX

Figure 1. The ACES CE for ATSHA204 screen

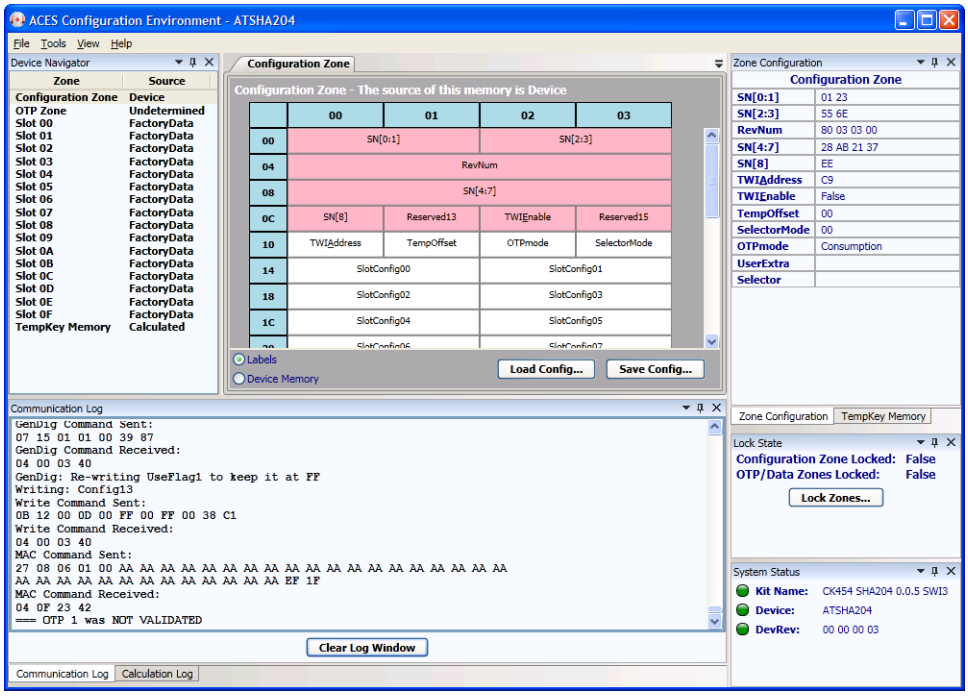

Figure 2. The ACES challeng-response demo screen

1. Introduction

This document provides an overview of the ACES and describes the major features in the ACES package. The ACES package is designed to minimize the learning curve when using the Atmel ATSHA204 and the Atmel ATAES132 CryptoAuthentication devices in your application. The package includes tools to help *educate* you as you begin to use the ATSHA204 and the ATAES132 devices, tools to *demonstrate* the ATSHA204 device in a typical authentication scenario, and tools to *configure* the ATSHA204 and the ATAES132 devices. These tools will assist you in designing and integrating the ATSHA204 and the ATAES132 devices into your system.

Educate

The integrated ACES help system includes:

- Help for the ACES applications
  - Configuration environment help
  - Challenge-response demo help
- Walkthroughs
  - Getting started guides
  - ACES user application guidance
- Application note index
  - Integrated and accessible user application scenarios
  - Select list of relevant application notes
- Datasheets
  - Integrated and accessible specification data

Demonstrate

The challenge-response demo offers a user-configurable simulation of the security provided by the ATSHA204 device:

- Animated system “enabled” or “disabled”
- Animated ATSHA204 device communication and status
- Device communication log
- Ability to configure the system key
- Context-sensitive help

Configure

The ACES CE allows you to easily configure devices for system design, prototyping, and small production runs. CE includes:

- Device zone layout
- Device memory visualization
- Zone configuration settings
- Device configuration
- Device locking
- Device command execution
- Device communication log
- System security calculation log
- Context-sensitive help

2. The ACES Package

2.1. ACES CE

The ACES CE (shown in Figure 1) provides you with a simple visualization of the device in a familiar, integrated development environment (IDE). Using the ACES CE requires a supported development kit, such as the Atmel ATAVRSECURITY kit, the Atmel AT88CK101 kit, Atmel AT88CK427 kit, or the Atmel AT88CK454 kit.

The “device navigator” shows a selectable list of all the zones on the ATSHA204 and the ATAEAS132 devices. The contents of the CE’s “zone map” and “zone configuration” panes are determined by the selection in the “device navigator.” The bytes in the ATSHA204 and the ATAES312 devices’ configurable locations can be modified by simply clicking in the zone map.

A “command builder” has been provided for exercising the ATSHA204 and the ATAES132 devices. The command builder provides access to all available commands, and provides the exact bytes that each command sends and receives.

Context-sensitive help, described below, is available everywhere in the ACES CE simply by pressing the F1 key from any screen, and so you are never too far from the information you needed.

2.2. ACES Challenge-response Demo

The ACES challenge-response demo exercises the ATSHA204 device in a typical authentication scenario. Using the ACES demo requires a supported development kit, such as the Atmel AT88CK101 kit, or the Atmel AT88CK454 kit.

The demo consists of two side-by-side windows (shown in Figure 1). The left window visualizes the state of the system; either “enabled” or “disabled.” The right window visualizes the communication with the ATSHA204 device, and also includes a communication log that shows the actual bytes sent to and received from the device.

The demo is interactive. When one of the supported development kits is plugged in, the demo application detects the kit and automatically sends a challenge to the ATSHA204 device. If the challenge is successful, the left window goes to its enabled state. When the kit is unplugged, the left window goes back to its disabled state. If the ATSHA204 device does not have the “system secret” programmed into it, the left window stays in the disabled state.

Context-sensitive help, described below, is available everywhere in the ACES demo simply by pressing the F1 key from any screen, and so you are never too far from the information you needed.

2.3. ACES Help

The ACES includes a comprehensive, context-sensitive help system, providing links from help topics directly to the relevant sections of the ATSHA204 or the ATAES132 datasheet when using the ACES CE and demo application. Further, integrated application notes and walkthroughs help to shorten the learning curve.

2.3.1. ACES CE Help

The ACES CE provides context-sensitive help for every window, dialog box, and menu. Since the ACES CE is designed to configure and exercise the ATSHA204 and the ATAES132 devices, the help topics have links directly to the relevant sections of the ATSHA204 and the ATAES132 datasheets. These direct datasheet links provide the information you need at your fingertips, minimizing the frustration and time spent searching the datasheet.

Pressing the F1 key from any screen in the ACES CE launches the context-sensitive help.

2.3.2. ACES Demo Help

The ACES demo also provides context-sensitive help for every window and dialog box. Since the ACES demo is designed to exercise the ATSHA204 device in an actual application scenario, the help topics have links directly to the relevant sections of the ATSHA204 datasheet. These direct datasheet links provide the information you need at your fingertips, minimizing the frustration and time spent searching the datasheet.

Pressing the F1 key from any screen in the ACES challenge-response demo launches the context-sensitive help.

2.3.3. Walkthrough Help

The ACES CE and ACES demo both have walkthrough help to provide a basic understanding of the ACES applications and the ATSHA204 and the ATAES132 devices. These include:

- The ACES CE getting started guide
- The ACES demo getting started guide
- A challenge-response walkthrough
- A system configuration walkthrough

2.3.4. Datasheet Help

The ATSHA204 and the ATAES132 datasheets are integrated into the ACES help system. This interlinked and searchable version of the datasheet exposes all the details of the ATSHA204 and the ATAES132 devices.

2.3.5. Application Note Help

An index of select application notes is integrated into the ACES help system. These application notes include topics that are relevant to system security, using the ATSHA204 and the ATAES132 devices, and designing the ATSHA204 and the ATAES132 devices into your system.

3. Revision History

Doc. Rev.	Date	Comments
8750A	05/2011	Initial document release

Atmel Corporation
2325 Orchard Parkway
San Jose, CA 95131
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 Road
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
9F, Tonetsu Shinkawa Bldg.
1-24-8 Shinkawa
Chuo-ku, Tokyo 104-0033
JAPAN
Tel: (+81)(3) 3523-3551
Fax: (+81)(3) 3523-7581

© 2011 Atmel Corporation. All rights reserved. / Rev.: 8750A–CRYPTO–5/11

Atmel®, logo and combinations thereof, and others are registered trademarks or trademarks of Atmel Corporation or its subsidiaries. Other terms and product names may be trademarks of others.

Disclaimer: The information in this document is provided in connection with Atmel products. No license, express or implied, by estoppel or otherwise, to any intellectual property right is granted by this document or in connection with the sale of Atmel products. EXCEPT AS SET FORTH IN THE ATMEL TERMS AND CONDITIONS OF SALES LOCATED ON THE ATMEL WEBSITE, ATMEL ASSUMES NO LIABILITY WHATSOEVER AND DISCLAIMS ANY EXPRESS, IMPLIED OR STATUTORY WARRANTY RELATING TO ITS PRODUCTS INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NON-INFRINGEMENT. IN NO EVENT SHALL ATMEL BE LIABLE FOR ANY DIRECT, INDIRECT, CONSEQUENTIAL, PUNITIVE, SPECIAL OR INCIDENTAL DAMAGES (INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS AND PROFITS, BUSINESS INTERRUPTION, OR LOSS OF INFORMATION) ARISING OUT OF THE USE OR INABILITY TO USE THIS DOCUMENT, EVEN IF ATMEL HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. Atmel makes no representations or warranties with respect to the accuracy or completeness of the contents of this document and reserves the right to make changes to specifications and products descriptions at any time without notice. Atmel does not make any commitment to update the information contained herein. Unless specifically provided otherwise, Atmel products are not suitable for, and shall not be used in, automotive applications. Atmel products are not intended, authorized, or warranted for use as components in applications intended to support or sustain life.