# imall

Chipsmall Limited consists of a professional team with an average of over 10 year of expertise in the distribution of electronic components. Based in Hongkong, we have already established firm and mutual-benefit business relationships with customers from, Europe, America and south Asia, supplying obsolete and hard-to-find components to meet their specific needs.

With the principle of "Quality Parts, Customers Priority, Honest Operation, and Considerate Service", our business mainly focus on the distribution of electronic components. Line cards we deal with include Microchip, ALPS, ROHM, Xilinx, Pulse, ON, Everlight and Freescale. Main products comprise IC, Modules, Potentiometer, IC Socket, Relay, Connector. Our parts cover such applications as commercial, industrial, and automotives areas.

We are looking forward to setting up business relationship with you and hope to provide you with the best service and solution. Let us make a better world for our industry!



## Contact us

Tel: +86-755-8981 8866 Fax: +86-755-8427 6832 Email & Skype: info@chipsmall.com Web: www.chipsmall.com Address: A1208, Overseas Decoration Building, #122 Zhenhua RD., Futian, Shenzhen, China





## Atmel CryptoAuthentication Evaluation Kit

Atmel AT88CK454BLACK Quick Start Guide

#### Features

- Installing Atmel CryptoAuthentication Evaluation Studio (ACES)
- Powering the board
- Reading the device configuration information Atmel ATSHA204 device

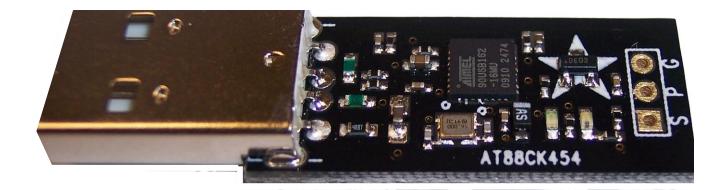
#### Introduction

#### Contents

- Atmel AT88CK454BLACK USB Dongle
- Quick start guide

Atmel<sup>®</sup> AT88CK454BLACK is an Atmel CryptoAuthentication<sup>™</sup> evaluation kit, which can be used as a reference design for an USB application requiring the Atmel CryptoAuthentication product family.

Figure 1. Atmel AT88CK454BLACK evaluation kit





1. Install ACES (Atmel CryptoAuthentication Evaluation Studio)

Visit www.atmel.com/cryptokits to download and install the latest ACES.

## 2. Powering up the board

The Atmel AT88CK454BLACK is a USB powered device.

• Simply insert the board into an open USB port

Figure 2-1. Atmel AT88CK454BLACK USB device



### 3. Reading the device configuration zone

- Insert the Atmel AT88CK454BLACK into a USB port
- Launch <u>ACES CE</u> for the desktop shortcut icon or from Start / All Programs / Atmel Crypto Solutions / ACES / ACES CE

Figure 3-1. ACES





• Figure 3-2 will appear indicating the board (CK454), device (SHA204), firmware version (0.0.5), communication interface (SWI - single wire interface), and the device lead count SWI<u>3</u>.

Figure 3-2. Kit detection screen

🐱 Kit Detection	? 🔀
The CK454 SHA204 0.0.5 SWI3 K detected Select Kit	iit has been
Show Quick Start Guide	

- Selecting the **Show Quick Start Guide** check box will launch the QSG alongside the configuration environment
- Click the "Select Kit" button to launch ACES Configuration Environment ATSHA204 pane

ACES Configurat	ion Environment	- ATSHA20	4							
<u>File Tools View H</u> e	lp									
Device Navigator • 4 × Configuration Zone					4	TempKey Memory	<b>≁</b> ‡ ×			
Zone	Source	Configuration Zone - The source of this memory is Device						TempKey Memory		
Configuration Zone Device		Conngura	coninguration zone - The source of this memory is device					TempKey Byte		
OTP Zone Slot 00	Undetermined FactoryData		00	01	02	03		KeyID	01	
Slot 01	FactoryData	00	00 SN[0:1] SN[2:3]		^	SourceFlag	Input			
Slot 02 Slot 03	FactoryData FactoryData						GenData CheckFlag	True False		
Slot 04	FactoryData	04		Rev	Num			Valid	True	
Slot 05 Slot 06	FactoryData FactoryData	08		SN[	4:7]			7010	1.100	
Slot 07 Slot 08	FactoryData FactoryData	0C	SN[8]	Reserved13	TWI <u>E</u> nable	Reserved15				
Slot 09 Slot 0A	FactoryData FactoryData	10	TWIAddress	TempOffset	OTPmode	SelectorMode				
Slot 0B Slot 0C	FactoryData FactoryData	14	SlotC	onfig00	SlotC	onfig01				
Slot 0D Slot 0E	FactoryData FactoryData	18	SlotC	onfig02	SlotC	onfig03				
Slot 0F TempKey Memory	FactoryData Calculated	10	SlotC	onfig04	SlotC	onfig05				
			Slot	onfia06	Slot	onfig07	~			
Communication Log		O Labels	lemory		Load Config	J Save Confi	g ▼ ậ X	Zone Configuratio	n TempKey Memory	
Detected Kit: CF Detected Kit: CF DevRev Command S 07 30 00 00 00 DevRev Command F 07 00 00 00 33 Read Command Rec 23 01 23 1B 3B A1 82 E0 A3 60 S Read Command Rec 07 02 00 00 00 3 Read Command Ser 07 02 00 00 00 3 Read Command Ser 07 01 23 1B 3B 7 Read Command Ser	<pre>K454 SHA204 0.0 sent: 13 5D teceived: 33 AP tt: 19 AD selved: 30 03 03 00 28 .44 40 A0 85 AP tt: LE 2D selved: 18 70</pre>	.5 SWI3 AB 21 37 1	55 00 FF C Clear Log V		0 80			Lock State Configuration : OTP/Data Zone Lock System Status Kit Name: Device:	÷ ᡎ × Zone Locked: False	
Communication Log	Calculation Log									
							j			

Figure 3-3. ACES Configuration Environment – Atmel ATSHA204



• All three **System Status** fields should be green and populated, which indicates the proper communication with the development kit and the Atmel ATSHA204 device

Kit Name:	SHA204 0.0.3 SWI
Device:	ATSHA204
DevRev:	00 00 00 03

## 4. Executing the Validate MAC Command

• Go to Tools \ Validate MAC to launch the Validate MAC window, see Figure 4-1

Figure 4-1.	Validate MAC tools menu
-------------	-------------------------

ACES Configuration Environment - ATSHA204								
File	Tools	View	Help		_			
Devic Write Zone • 4 × Command Builder ce				Configuratio				
Con		date M				Co	onfigur	ation
OTP Slot Slot	Edit		ermission	s	mined )ata )ata		00	
Slot Slot Slot	03		Fac	tory	Data Data Data		04	
Slot Slot	06		Fac	tory	Data Data		08	
Slot Slot Slot	08		Fac	tory	Data Data		0C	
Slot	0A		Fac	tory	Data Data		10	Т
Slot Slot	0C		Fac	tory	Data Data		14	
Slot Slot	0E		Fac	tory	Data Data		18	
Slot Tem	0F IpKey I	1emor		tory culat	Data :ed		10	
						0	Labels	

- Figure 4-2 will appear
- Click the Execute Nonce button
- Click the MAC button
- Click the CheckMac button
- The CheckMac Result: should indicate Matched



#### Figure 4-2. Validate MAC pane

Validate MAC	
Nonce	
Challenge	41.525
Type Challenge Here	Text
Challenge Bytes 54 79 70 65 20 43 68 61 6C 6C 65 6E 67 65 20 48 65 72 65 00	
Nonce RandOut - (combined with "Challenge" to produce TempKey)	
FF FF 00 00 FF FF 00 00 FF FF 00 00 FF FF	FF 00 00 FF FF 00 00
ТетрКеу	
1E DC CA A0 20 88 6A E8 47 57 99 7A 53 8A 2D 04 DC 72 77 3A AC E9 41 49 0D 4	1 49 58 06 7C ED 45
TempKey.Valid: False	
MAC	
Key ID 0	
MAC Response Matched	
	SD BC DA 16 B2 96 17
CheckMac	
Key ID 0	
Client Challenge 1E DC CA AO 20 88 6A E8 47 57 99 7A 53 8A 2D 04 DC 72 77 3A AC E9 41 49 0D 4	41 49 58 06 7C ED 45
Client Response	
01 D1 A7 0A 78 26 F3 B1 E6 0B 83 D4 C6 76 37 D3 E5 E7 77 BC 6B A6 27 BA 51 5	5D BC DA 16 B2 96 17
Execute CheckMac	
CheckMac Result: Matched	
Execute Nonce, MAC, & CheckMac	

Congratulations, your Atmel AT88CK454BLACK is up and running. See ACES online Help additional information. For additional samples, go to: http://www.atmel.com/forms/Samples.asp?family\_id=699

#### 5. Additional Kits Information

Table 5-1.	Atmel C	CryptoAuthentication	kits
------------	---------	----------------------	------

Atmel CryptoAuthentication kits					
Atmel kits	Atmel device supported	Device footprint	Socket(s)		
AT88CK454BLACK	ATSHA204	SOT23-3	None/USB Dongle		
AT88CK101STK3	ATSHA204	SOT23-3	1		
AT88CK101STK8	ATSHA204	8LD SOIC	1		
AT88CK109STK3	ATSHA204	SOT23-3	2		
AT88CK109STK8	ATSHA204	8LD SOIC	2		

## 6. Firmware upgrade

See application note, doc8746, Upgrading Crypto Kits Firmware.



## 7. References and further information

A complete reference design including schematics, Gerber files, bill of materials (BOM), hardware user guide and development and demonstration software is conveniently downloadable from the Atmel website at www.atmel.com/cryptokits.

## 8. EVALUATION BOARD/KIT IMPORTANT NOTICE

This evaluation board/kit is intended for **ENGINEERING**, **DEVELOPMENT**, **DEMONSTRATION** or **EVALUATION PURPOSE ONLY**. It is not a finished product and may not (yet) comply with some or any technical or legal requirements that are applicable to finished products, including, without limitations, directives regarding electromagnetic compatibility, recycling (WEEE), FCC, CE or UL (except as may be otherwise noted on the board/kit). Atmel<sup>®</sup> supplied this board/kit "AS IS," without any warranties, with all faults, at the buyer's and further users' sole risk. The user assumes all responsibly and liability for proper and safe handling of goods. Further, the user indemnifies Atmel from claims arising from the handling or use of goods. Due to open construction of the product, it is the user's responsibility to take any and all appropriate precautions with regard to electrostatic discharge and any other technical or legal concerns.

EXCEPT TO THE EXTENT OF INDEMNITY SET FORTH ABOVE, NEITHER USER NOR ATMEL SHALL BE LIABLE TO EACH OTHER FOR ANY INDIRECT, SPECIAL, INCIDENTAL, OR CONSEQUENTIAL DAMAGES.

No license is granted under any patent right or other intellectual property right of Atmel covering or relating to any machine, process, or combination in which such Atmel product or services might be or are used.

Mailing Address: Atmel Corporation 2325 Orchard Parkway San Jose, CA 95131



#### **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.: 8724A-CRYPTO-3/11

Atmel<sup>®</sup>, logo and combinations thereof, CryptoAuthentication<sup>™</sup> 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 INCIDENTIAL 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.