

Atmel CryptoAuthentication Starter Kit

Atmel AT88CK101STK8 Quick Start Guide

Features

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

Contents

- Atmel AT88CK101BK8 daughter board
- Atmel AT88Microbase AVR base module
- 6" USB cable
- Atmel ATSHA204 samples

Introduction

Atmel[®] AT88CK101STK8 is an Atmel CryptoAuthentication[™] starter kit, which can be used as a reference design for an USB application requiring the Atmel CryptoAuthentication product family.

Figure 1. Atmel AT88CK101STK8 starter kit





1. Install ACES (Atmel CryptoAuthentication Evaluation Studio)

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

2. Configuring the Atmel AT88CK101BK8 and Atmel AT88Microbase boards

- Ensure the Atmel ATSHA204 device in place in the socket with the correct Pin1 orientation
- The K1 switch on the Atmel AT88CK101BK8 board should always be in the "uBase" position when mounted to the Atmel AT88Microbase
- The 8ld SOIC package supports both SWI (Single Wire Interface) and I²C communication protocol. The following steps configure the kit for I²C communication, since the samples in this kit are shipped with I²C enabled.



Figure 2-1. Atmel AT88CK101BK8 CryptoAuthentication daughter board

• The K1 switch on the Atmel AT88CK101BK8 board should always be in the "uBase" position when mounted to the Atmel AT88Microbase

Figure 2-2. Atmel AT88Microbase with an Atmel AT90USB1287 AVR





Table 2-1. Configuration table

Configuration table							
Communication protocol	Atmel AT88CK101BK8 (K1 switch setting)	Atmel AT88Microbase (K1 switch setting)	Comments				
I ² C	uBase	TWI (I ² C)	Kit shipped with this setup				
SWI	uBase	SPI					

3. Powering up the board

The Atmel AT88CK101STK8 is a USB powered device.

• Simply insert the board into an open USB port

Table 3-1. Atmel AT88CK101STK8 USB powered





4. Reading the device configuration zone

- Insert the Atmel AT88CK101STK8 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 4-1. ACES



• Figure 4-2 will appear indicating the board (CK101), device (SHA204), firmware version (0.0.6), and the communication interface (TWI)

Figure 4-2. Kit detection screen

💀 Kit Detection	? 🔀
The CK101 SHA204 0.0.6 TWI Ki detected	t 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



Toon Tren II	lelp									
evice Navigator	~ ↓ ×	Configu	ration Zone				Ŧ	Zone Configuratio	on 🔻 🕂 🕽	
Zone	Source						Configuration Zone			
Configuration Zone	Device	Configura	tion Zone - The	source of this me	mory is Device			SN[0:1]	01 23	
TP Zone	Undetermined		00	01	02	03		SN[2:3]	59 BD	
lot 00	FactoryData							RevNum	80 03 03 00	
lot 01	FactoryData	00	SN	[0:1]	SN	[2:3]		SN[4:7]	29 AB 21 37	
ot 03	FactoryData	04		Revi	lum			SN[8]	EE	
ot 04	FactoryData	04						TWIAddress	C8	
ot 05	FactoryData	08		SN[4	4:7]			TWIEnable	True	
ot 07	FactoryData				and the second second	-		TempOffcet	00	
ot 08	FactoryData	OC	SN[8]	Keserved13	IWIEnable	Keserved15		SelectorMode	00	
ot 09	FactoryData	10	TWIAddress	TempOffset	OTPmode	SelectorMode		OTPmode	Consumption	
t OA	FactoryData				1040.000.0000			UconExten	consumption	
ot OC	FactoryData	14	SlotC	onfig00	SlotC	onfig01		Calastas		
ot OD	FactoryData		clase		ci-to			Selector		
ot OE	FactoryData	18	3000	oningoz	51000	oningos				
Slot OF FactoryData TempKey Memory Calculated 1C SlotConfig04 SlotConfig05		1C	SlotConfig04 SlotConfig05		onfig05					
mmunication Log	1	<u>.</u>					• ₽ ×	Zone Configural	tion TempKey Memory	
enDig Command	Sent: 39.87						^	Lesson and the second		
enDig Command	Received:							Lock State	• µ	
00 03 40								Configuration	Tone Locked: False	
enDig: Re-writ	ting UseFlag1 to	keep it a	t FF					OTP/Data Zo	nes Locked: False	
riting: Config	jij Sent:							Lo	ck Zones	
WFILE COMMAIN SENT: 0B 12 00 0D 00 FF 00 FF 00 38 C1									6.6	
3 12 00 0D 00	leceimed:									
3 12 00 0D 00 rite Command R	received:									
5 12 00 0D 00 rite Command R 1 00 03 40	eceiveu:					MAC Command Sent:				
8 12 00 0D 00 rite Command R 8 00 03 40 8 C Command Sen 9 08 06 01 00	nt:		, ,, ,, ,, , , ,,	** ** ** ** *	N NN					
3 12 00 0D 00 rite Command R 1 00 03 40 AC Command Sen 7 08 06 01 00 A AA AA AA AA	nt: AA AA AA AA AA AA AA AA AA AA AA A	AA AA AA <i>A</i> AA AA AA E	A AA AA AA AA F 1F	. AA AA AA AA A	A AA			System Status	▲ İ	
5 12 00 0D 00 rite Command R 4 00 03 40 AC Command Sen 7 08 06 01 00 A AA AA AA AA AC Command Rec	nt: AA AA AA AA AA AA AA AA AA AA AA A ceived:	aa aa aa a aa aa aa e	A AA AA AA AA F 1F	. AA AA AA AA A	A AA			System Status		
5 12 00 0D 00 rite Command R 4 00 03 40 AC Command Sen 7 08 06 01 00 A AA AA AA AA AC Command Rec 4 0F 23 42	ht: AA AA AA AA AA AA A AA AA AA AA AA A ceived:	AA AA AA A AA AA AA E	A AA AA AA AA F 1F	. AA AA AA AA A	A AA		_	System Status Kit Name: Device: 		
5 12 00 0D 00 Fite Command R 4 00 03 40 C Command Sen 08 06 01 00 AA AA AA C Command Rec 4 0F 23 42 = OTP 1 was N	ht: AA AA AA AA AA AA AA AA AA AA AA A seived: NOT VALIDATED	AA AA AA A AA AA AA E	A AA AA AA AA F 1F	. aa aa aa aa a	A AA		4	System Status Kit Name: Device: DevRev:	→ 和 CK101 SHA204 0.0.6 TWI ATSHA204 00 00 00 03	
b 12 00 0D 00 rite Command R 4 00 03 40 AC Command Sen 7 08 06 01 00 A AA AA AA AA AC Command Rec 4 0F 23 42 == OTP 1 was N	ALCEIVED: AA AA AA AA AA AA AA AA AA AA AA A Seived: NOT VALIDATED	AA AA AA A AA AA AA E	A AA AA AA AA F 1F Clear Log W	. AA AA AA AA AA	A AA		E.	System Status Kit Name: Device: DevRev:	 	

Figure 4-3. ACES configuration environment – 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:	CK101 0.0.6 TW
Device:	ATSHA204
DevRev:	00 00 00 03

5. Executing the Validate MAC command

- Go to Tools $\$ Validate MAC to launch the Validate MAC window, see Figure 5-1



Figure 5-1. Validate MAC tools menu



- Figure 5-2 will appear
- Click the Execute Nonce button
- Click the MAC button
- Click the CheckMac button
- The CheckMac Result: should indicate Matched

Figure 5-2. Validate MAC pane

Validate MAC					
Nonce					Contract Contract Contract
Challenge					1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1
Type Challenge Here					Text
Challenge Bytes 54 79 70 65 20 43 68 61 6C 6C 65 6E 67 6	55 20 48 65 72 65	00			
	Execute Nonce				
Nonce RandOut - (combined with "Challenge" to	produce TempKey)				
FF FF 00 00 FF FF 00 00 FF FF 00 00 FF I	FF 00 00 FF FF 00	00 FF FF 0	0 00 FF FF	00 00 FF	FF 00 00
TempKey					
1E DC CA AO 20 88 6A E8 47 57 99 7A 53 8	A 2D 04 DC 72 77	3A AC E9 41	49 00 41	49 58 06	7C ED 45
TempKey.Valid: False					
MAC		_			
	ACES Message	X			
MAC Response 01 D1 A7 0A 78 26 F3 81 66 08 83 D4 C6	Matchee	d 68 A6 2	7 BA 51 50	BC DA 16	B2 96 17
CheckMac		8 J.			
Key ID 0					
Client Challenge					
1E DC CA A0 20 B8 6A E8 47 57 99 7A 53 1	8A 2D 04 DC 72 77	3A AC E9 4	L 49 0D 41	49 58 06	7C ED 45
Client Response					
01 D1 A7 0A 7B 26 F3 B1 E6 0B 83 D4 C6 3	76 37 D3 E5 E7 77	BC 68 A6 2	7 BA 51 50	BC DA 16	B2 96 17
	Execute CheckMa	ac			
CheckM	ac Result:	Match	ed		
Execute	Nonce, MAC, &	CheckMac			



Congratulations, your Atmel AT88CK101STK8 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

6. Additional Kits Information

Table 6-1. Atmel CryptoAuthentication kits

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

7. Firmware Upgrade

See application note, doc8746, Upgrading Crypto Kits Firmware.

8. 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.



9. 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[®] 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

 \odot 2011 Atmel Corporation. All rights reserved. / Rev.: 8738A–SMEM–3/11

Atmel[®], logo and combinations thereof, CryptoAuthentication[™] 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 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.