DM320109

CryptoAuthentication™ Xplained-Pro Starter Kit User Guide

Introduction

The CryptoAuthentication Xplained Pro Starter Kit (CryptoAuth-XSTK) is the newest addition to the CryptoAuthentication evaluation kits. This kit is used for exploring and interfacing CryptoAuthentication devices in Windows®, Linux® and Mac® environments. This kit performs the same functionality as the AT88CK101 family of kits but provides additional features. This user guide provides a physical overview and connections and details of the kit working with the Atmel Crypto Evaluation Studio (ACES) application.
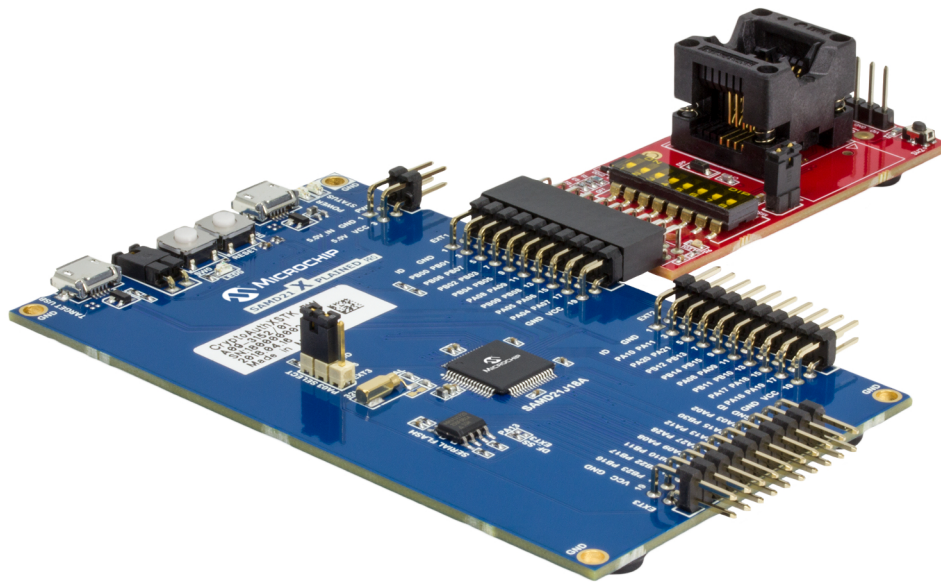
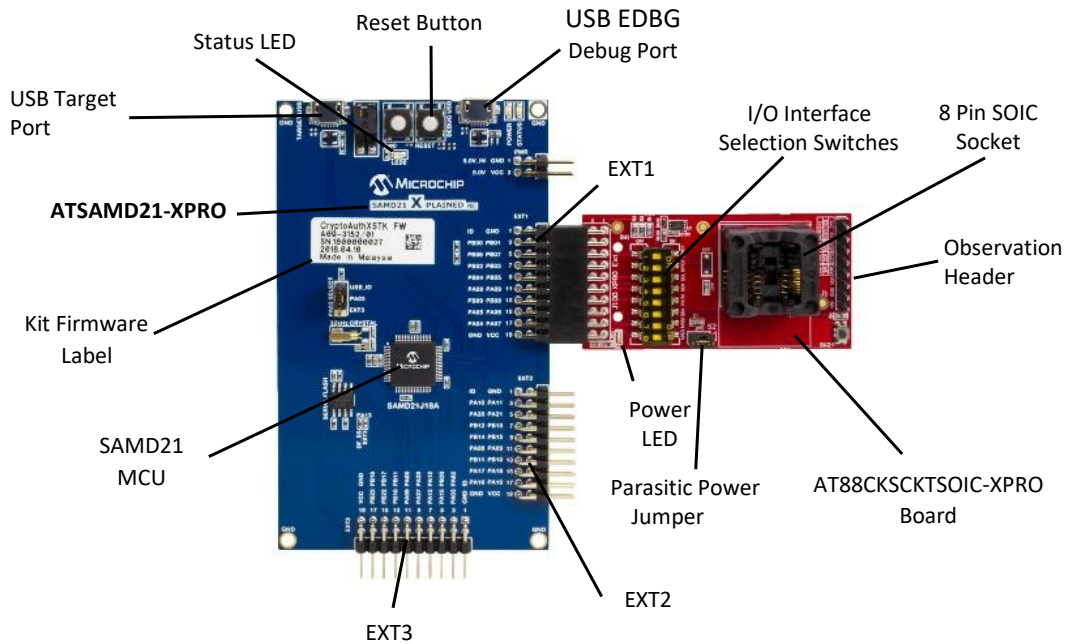**Figure 1. CryptoAuthentication™ SOIC Starter Kit**

Table of Contents

1.   Overview

The kit consists of the SAMD21 Xplained Pro board and the AT88CKSCKTSOIC-XPRO socket board. The SAMD21-XPRO is pre-programmed with Microchip's Security Products Group (SPG) kit protocol. This protocol takes care of the communication between the CryptoAuthentication devices and the host system regardless of the device interface. The data transfer between the kit and the PC is indicated by the Status LED on the SAMD21 board.

Figure 1-1. Key Kit Features

2. Software and Hardware Requirements

The following describes the requirements for using the CryptoAuthentication Starter Kit with ACES.

2.1 Software

- **ACES Rev 6.0.3 (Or higher)**
  The ACES package is a suite of PC-based software tools to configure and demonstrate the Microchip CryptoAuthentication family of devices. Versions of ACES prior to 6.0.3 will not recognize the CryptoAuth-XSTK kit. For firmware updates refer to Section Firmware Upgrade of this document.

- **Serial Console Software (Optional)**
  Applications like TeraTerm, Putty or equivalents can be used for data logging and for monitoring the data packets between the kit and the PC

2.2 Hardware

- ATSAMD21-XPRO - Xplained Pro Evaluation Kit with SAM D21 ARM® Cortex®-M0+ microcontroller
- AT88CKSCKTSOIC-XPRO extension board with 8-pin SOIC Socket
- CryptoAuthentication ICs - Any IC from the compatible list
- Two Micro-B to Type-B USB Interface cables (one for PC and one for Data logging (Optional)); only one USB cable is provided in the kit

3. Getting Started With ACES

ACES provides a way to explore the structure and operation of individual CryptoAuthentication devices. The tool will work with all CryptoAuthentication devices with all I/O modes of operation. The following sections detail how to initially set up the hardware to run ACES and then demonstrate a simple operation in ACES using the Command Builder Tool.

1. Insert one of the provided CryptoAuthentication ICs into the socket of the AT88CKSCKTSOIC-XPRO board.

2. Change the I/O Interface Selection Switches on the top side of the AT88CKSCKTSOIC-XPRO to match with selected IC interface.
   - Refer to the bottom side of the AT88CKSCKTSOIC-XPRO to match with selected interface.

> ⚠️**WARNING**   It is required to select the correct I/O interface, otherwise communication with the device will fail.

3. Connect the AT88CKSCKTSOIC-XPRO to EXT1 or EXT2 extension header port of ATSAMD21-XPRO board. Note that AT88CKSCKTSOIC-XPRO board should not be connected to EXT3 header.

4. Connect USB cable between the TARGET USB of the ATSAMD21-XPRO board and the PC.
   Note: If a serial terminal application is not being used, then go to step 8.

5. Optionally, to monitor data packets transfer between the PC and SAMD21-XPRO board, connect the second USB cable between the USB EDBG Debug port of the SAMD21-XPRO board and the PC.

6. Open the serial terminal application such as TeraTerm or Putty, configure and open the port Atmel Corp EDBG USB Port for 115200 baud with 8 data bits, no parity and 1 stop bit. After the port is opened, any further data transfer between the PC and SAMD21-XPRO should be seen on the terminal.

7. Press the **RESET** button on the SAMD21-XPRO board to show the list of connected I^{2}C, SWI or the SPI devices.

Figure 3-1. Device Discovery Process
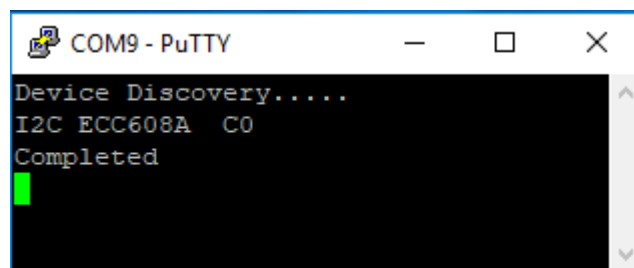
For this example, an ATECC608A with an I^{2}C interface was loaded into the socket. The output log is independent of the software used (see Section Other Supported Software). The output log also shows any communication errors.

8. Execute the ACES application in the PC and the application should list the discovered device(s).

Figure 3-2. ACES Device Detection
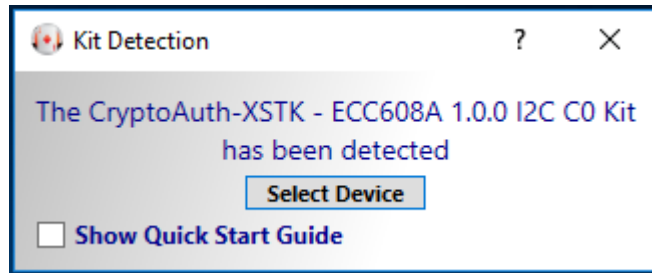
- If multiple boards are connected to EXT1 or EXT2, then both would be detected. The user needs to select between the devices shown.
- If a multi-device board is connected, then all the devices on that board will be detected and the user needs to select between the devices shown.

9. Click the **Select Device** button to initialize the ACES application with the device. The ACES application reads all the configuration data from the device and populates it as shown in Figure 3-3.

Figure 3-3. ACES Interface with the ATECC608A in I²C Mode
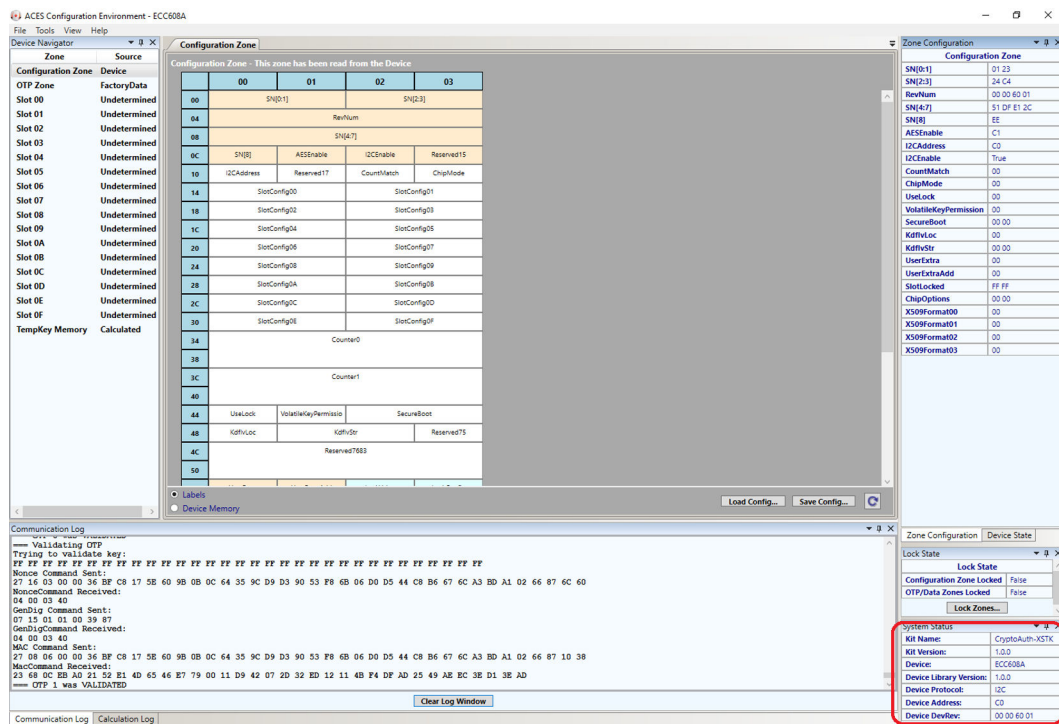
- The highlighted data in the above figure is the current device connected, its interface and its revision number.
- If the Serial Console is open, the user will be able to see all the data packets transfer between the kit and the ACES application.

3.1 Example using ACES Command Builder

1. Follow the procedure specified in the Getting Started with ACES Section.
2. From ACES menu bar, select *Tools>Command Builder*. From the Command Builder window, select the opcode and other information, then click the **Execute Command** button. ACES should be able to send the command to the kit and receive the data from the kit.

Figure 3-4. Command Builder for Info Command
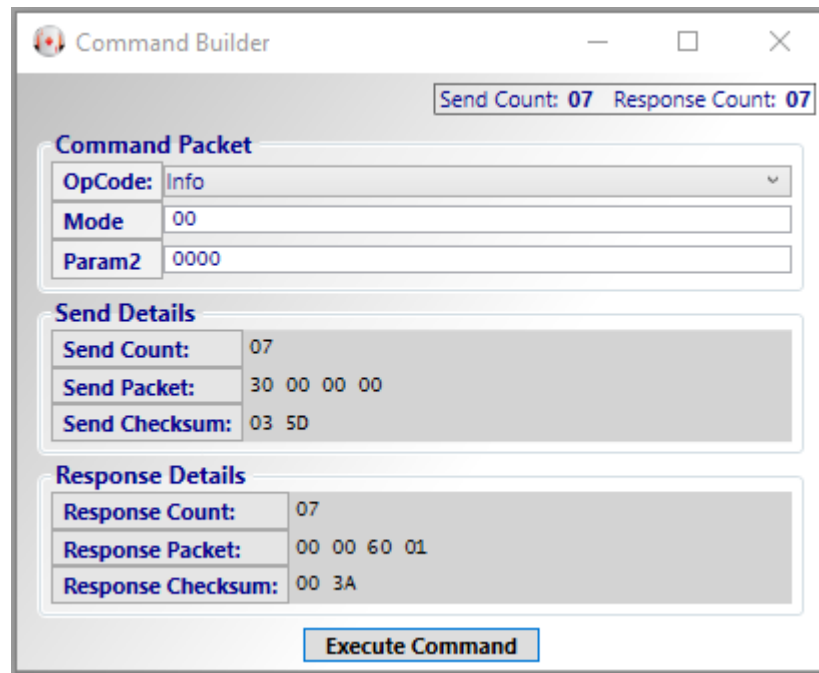
Figure 3-5. Info Command Displayed on Serial Console
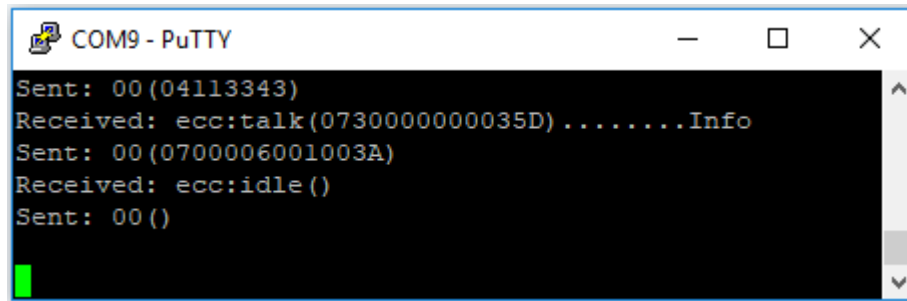
Important Notes:

1. The AT88CKSCKTSOIC-XPRO boards or other compatible boards can be connected to both the EXT1 and EXT2 ports simultaneously.

2. The I^2C connection between EXT1 and EXT2 is the same bus. Two or more devices with same I^2C address connected on EXT1 and EXT2 will result in unpredictable operation.

3. If the AT88CKSCKTSOIC-XPRO or other board is connected after the ATSAMD21-XPRO board is powered, the user must press the **RESET** button on the ATSAMD21-XPRO board in order for the correct devices to be detected.

4. If the device in the socket is swapped out while the board is powered then the **RESET** button must be pressed in order for the correct device to be detected.

4. Other Supported Software

The previous sections explained how the kit will work with the ACES application. The kit firmware is designed to be flexible and work with other Microchip Secure Products tools and libraries. The core of the kit firmware is based on Microchip's Kit Protocol.

4.1 Kit Protocol

The Kit Protocol provides a mechanism to abstract and simplify the sending of commands from a host system. The Kit Protocol has several types of commands and identifiers used to communicate with a device that contains the Kit Protocol. These include:

1. System Level Commands that:
   - Identify the board
   - Identify firmware revision of the board
2. Device Level Commands that:
   - Identify or setup communication to the device
   - Allow for device identification
3. Generic Command Sequences
   - To pass specific commands to the device
   - To poll or read data back from a device

4.2 Additional Software Support

- **CryptoAuthLib-Python Module**
  Cryptoauthlib-Python is a Python® package with integrated Cryptoauthlib library. This package includes an application example and is supported in Windows, Linux and in Mac. This software is designed to make it easier to develop a host application by emulating the host through Python.

- **Host Projects**
  Any host project which supports USB HID and Kit Protocol can be interfaced with this kit. Windows HID Hardware Abstraction Layer (HAL), Linux HID HAL and Kit Protocol are supported in the Cryptoauthlib library. The projects created from the above HAL and Kit Protocol can also be used to interact with this kit.

5. Xplained Pro Extension Kit Compatibility

The AT88CKSCKTSOIC-XPRO is one of several Xplained Pro Extension kits that are used to support Microchip security products. Several other kits are currently available and additional kits may be developed in the future to support additional devices or package styles. The following kits are also compatible with the SAMD21-XPRO kit.

- **AT88CKSCKTUDFN-XPRO**
  This is a UDFN socket board with all of the same features as the AT88CKSCKTSOIC-XPRO board. This board is specifically designed for the customers who wish to develop with UDFN socket devices.

- **ATCryptoAuth-XPRO**
  The ATCryptoAuth-XPRO board has the ATECC508A, the ATSHA204A and the ATAES132A CryptoAuthentication devices. Each of these devices have an I^2C interface. Because each of these devices have a unique I^2C address, all three will be detected by the kit protocol firmware and by ACES.

- **ATCryptoAuth-XPRO-B**
  The ATCryptoAuth-XPRO-B board has all the same devices as the ATCryptoAuth-XPRO plus the ATECC608A. An onboard jumper is used to select either the ATECC508A or ATECC608A devices. If one of the ECC devices I^2C Address is changed and an additional jumper is used, then both devices can be detected.

6. AT88CK101 Compatibility

The CryptoAuthentication Starter Kit with the respective socket kit is intended to replace the AT88CK101 family of kits. Future development on the AT88CK101 kits is not planned. Firmware upgrades to correct critical issues may continue to be supported for a period of time. The following table provides a compatibility guide of support for the various AT88CK101 kits.

Table 6-1. CK101 Replacement Kits

CK101 Kit	CryptoAuth Starter Kit	Comments
AT88CK101SK-SSH-XPRO	DM320109	Direct Replacement
AT88CK101SK-MAH-XPRO	• DM320109+AT88CKSCKTUDFN-XPRO • ATSAMD21-XPRO +AT88CKSCKTUDFN	• If first option selected, then the UDFN socket can be used instead of the SOIC socket. • If second option selected will need to acquire samples and program the SAMD21. • For both of these options, UDFN sample devices will need to be acquired separately.
AT88CK101SK-RBH	Contact Microchip Sales	RBH Socket Board is currently planned for development.
AT88CK101STK3	No planned replacement	SOT23 package is only used for ATSHA204A.
AT88CK101SK-TSU-XPRO	No planned replacement	TSSOP package is only used for SHA204A and is not recommended for new designs.

6.1 CryptoAuthentication Starter Kit Feature Enhancements

- Direct support for CryptoAuth-XPRO and CryptoAuth-XPRO-B board
- Identification of up to eight CryptoAuthentication devices
  - Includes devices with mixed interfaces
  - Up to two SWI devices can be detected if on separate extensions
  - Up to two SPI devices can be detected if on separate extensions
  - Up to eight I^2C devices but all must have a unique I^2C address for proper operation
- Serial terminal support for monitoring operation
- Support for running devices in parasitic Power mode when using the socket kits
- Support for intrusion detection testing when using the UDFN or SOIC socket kits
- SWI GPIO mode support either through XPRO interface or observation header

6.2 CryptoAuthentication Starter Kit Operational Differences

- Kit will be identified as CryptoAuth-XSTK in ACES.

- No longer continuously polls for devices. When new devices are swapped in, the **RESET** button on the SAMD21 needs to be pressed to do discovery.
- Switches on socket board must always be set prior to operation.

7. Firmware Upgrade

The following sections detail the software, hardware, and procedure for upgrading the firmware of the kit.

7.1 Software and Hardware Prerequisites

Software Prerequisites:

- **Atmel Studio 7**
  Studio 7 is the integrated development platform (IDP) for developing and debugging all AVR$^®$ and SAM microcontroller applications. The Atmel Studio 7 IDP gives the user a seamless and easy-to-use environment to write, build and debug your applications written in C/C++ or assembly code. It also connects seamlessly to the debuggers, programmers and development kits that support AVR and SAM devices.

Hardware Prerequisites:

- ATSAMD21 Xplained Pro Evaluation Board
- One Micro-B to Type-B USB interface cable

7.2 Firmware Upgrade of the ATSAMD21-XPRO board.

The following procedure works for programming a default SAMD21-XPRO or for upgrading a SAMD21-XPRO that has been programmed with the CrypotAuth-XSTK firmware.

1. Connect the USB Cable from the PC to the "Debug USB" Port of the ATSAMD21 Xplained Pro board.
2. Start the Atmel Studio Application from the Start menu. The application should start and detect the ATSAMD21 Xplained Pro board as shown in Figure 7-1

Figure 7-1. Atmel Studio with ATSAMD21 Xplained Pro Board Detected
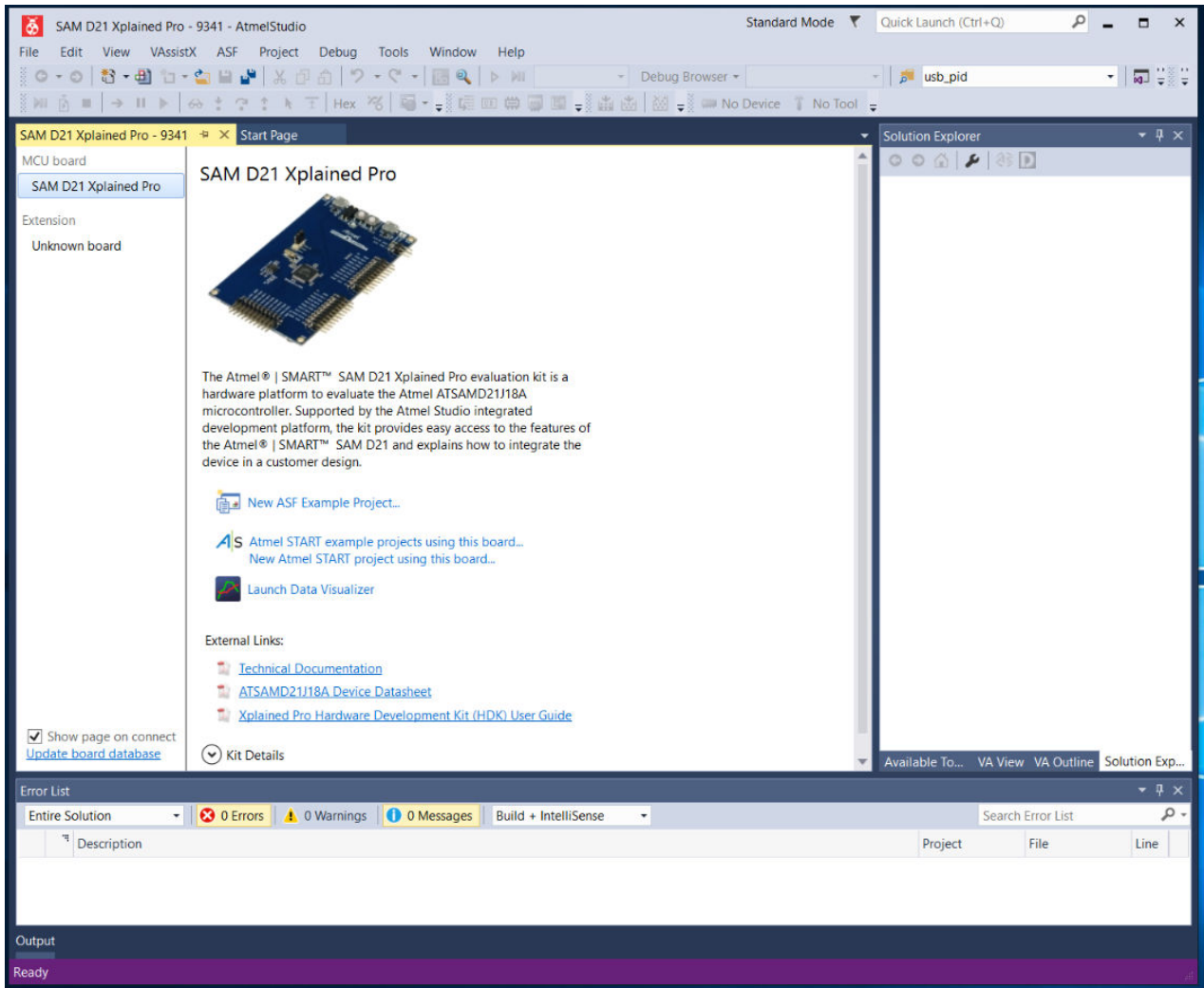
3. From the Tools menu, select **Device Programming** and the Device Programming window appears.

4. From the Device Programming window, select Tool as EDBG XXXXXXXXXXXXXX, select Device as ATSAMD21J18A, Interface as SWD. Click the **Apply** button. The results seen are the same as in

Figure 7-2. Device Programming Window with Tool, Device and Interface Selected.
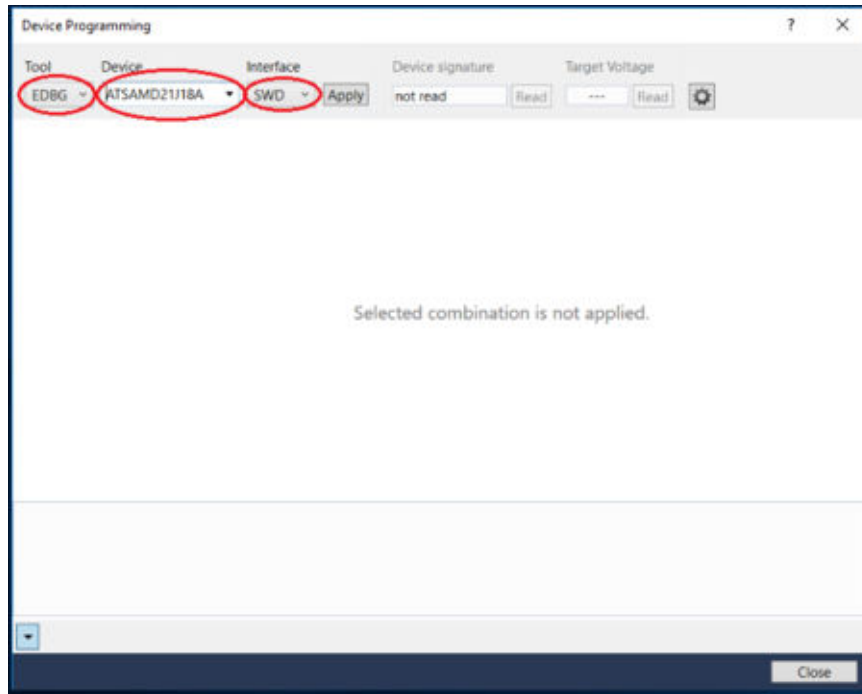
5. Click the **Read** button below the Device Signature and it reads the device signature and target voltage from ATSAMD21 Xplained Pro board and populates it in the corresponding text box as highlighted in Figure 7-3 This verifies the board is operating and communicating correctly.

Figure 7-3. Device Programming Window reading the Device Signature, Target Voltage and Device ID.
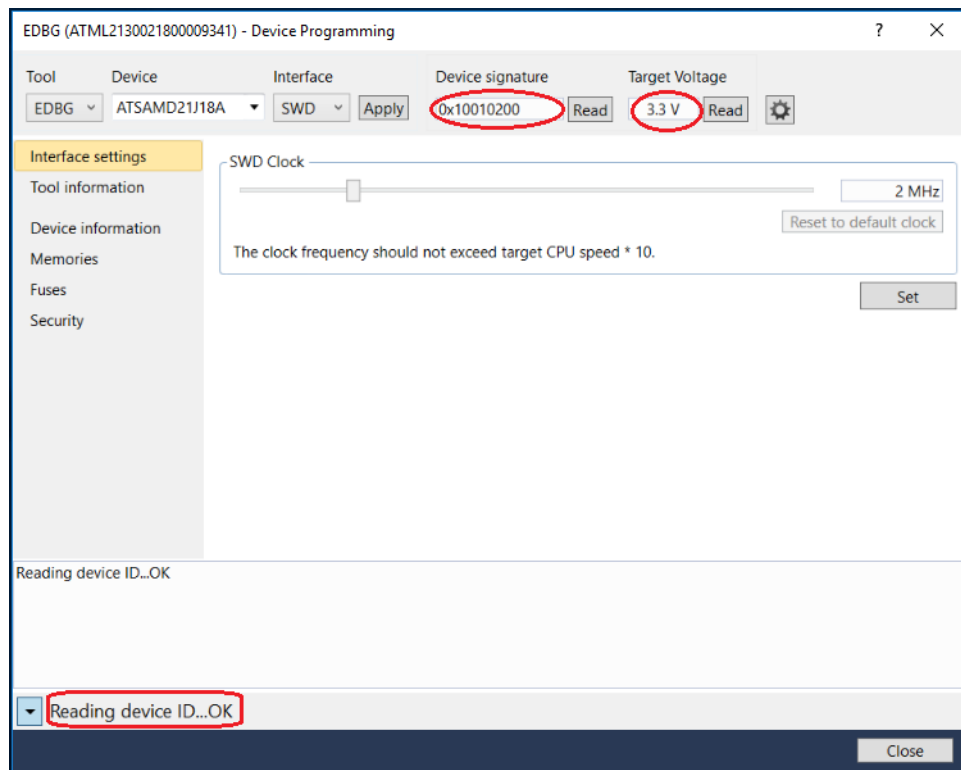
6. If the communication with the board was successful, select the firmware `cryptoauthxstk_vx.x.x.elf` (marked as 1 in Figure 7-4) from the location where ACES was installed. Then, click the **Program** button (marked as 2 in Figure 7-4).

Figure 7-4. Device Programming Window after Programming
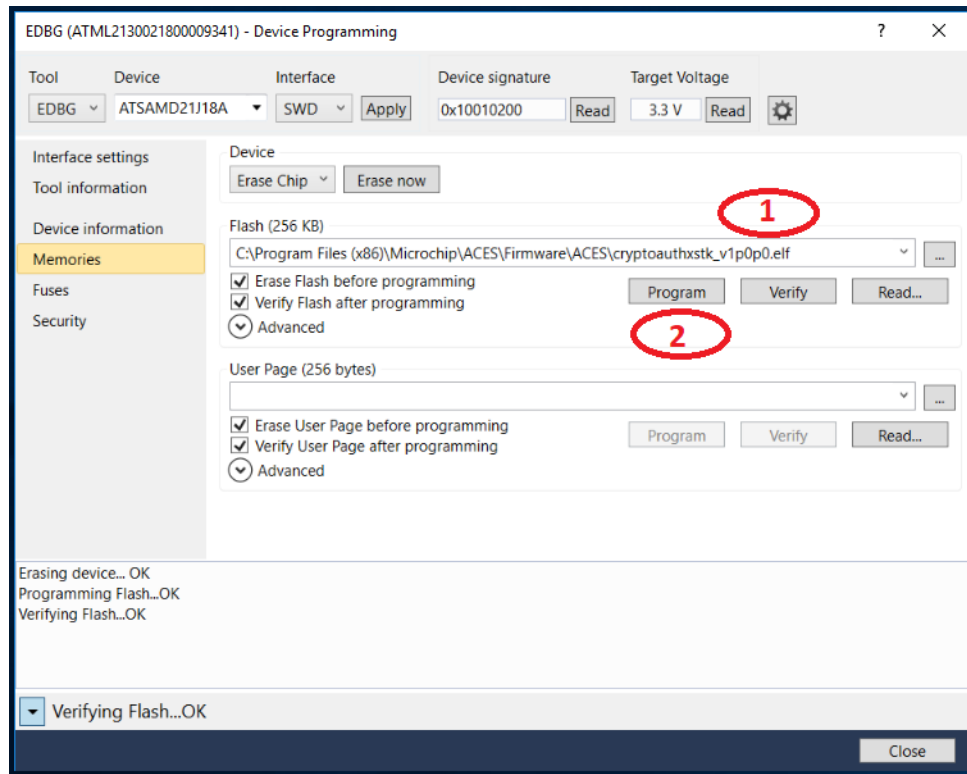
When the program button is clicked, it erases the old firmware, writes the new firmware and verifies the program written to the ATSAMD21 Xplained Pro board. The bottom left in Figure 7-4 shows the progress for the erasing the device, programming the Flash and verifying the Flash.

8.   Design Documentation

This section contains reference links to the schematics, PCB layouts, Gerber Files and Bill of Materials (BOM) for the ATSAMD21-XPRO and the AT88CKSCKTSOIC-XPRO kits.

ATSAMD21-XPRO

- Design Documentation (Schematics, Layer Plots, BOM, Gerber Files)

AT88CKSCKTSOIC-XPRO

- Design Documentation (Schematics, Layer Plots, BOM)
- Gerber Files

9.   References

The following is a list of additional references that may be useful when using this kit.

1. Microchip CryptoAuthentication Devices
2. CryptoAuthentication SOIC Starter Kit
3. ACES Software Package
4. Cryptoauthlib
5. AT88CKSCKTSOIC-XPRO
6. AT88CKSCKTUDFN-XPRO
7. ATCRYPTOAUTH-XPRO-B
8. ATCRYPTOAUTH-XPRO

10.   Document Revision History

Revision A (June 2018)

- Initial release of this document

The Microchip Web Site

Microchip provides online support via our web site at http://www.microchip.com/. This web site is used as a means to make files and information easily available to customers. Accessible by using your favorite Internet browser, the web site contains the following information:

- **Product Support** – Data sheets and errata, application notes and sample programs, design resources, user's guides and hardware support documents, latest software releases and archived software
- **General Technical Support** – Frequently Asked Questions (FAQ), technical support requests, online discussion groups, Microchip consultant program member listing
- **Business of Microchip** – Product selector and ordering guides, latest Microchip press releases, listing of seminars and events, listings of Microchip sales offices, distributors and factory representatives

Customer Change Notification Service

Microchip's customer notification service helps keep customers current on Microchip products. Subscribers will receive e-mail notification whenever there are changes, updates, revisions or errata related to a specified product family or development tool of interest.

To register, access the Microchip web site at http://www.microchip.com/. Under "Support", click on "Customer Change Notification" and follow the registration instructions.

Customer Support

Users of Microchip products can receive assistance through several channels:

- Distributor or Representative
- Local Sales Office
- Field Application Engineer (FAE)
- Technical Support

Customers should contact their distributor, representative or Field Application Engineer (FAE) for support. Local sales offices are also available to help customers. A listing of sales offices and locations is included in the back of this document.

Technical support is available through the web site at: http://www.microchip.com/support

Microchip Devices Code Protection Feature

Note the following details of the code protection feature on Microchip devices:

- Microchip products meet the specification contained in their particular Microchip Data Sheet.
- Microchip believes that its family of products is one of the most secure families of its kind on the market today, when used in the intended manner and under normal conditions.
- There are dishonest and possibly illegal methods used to breach the code protection feature. All of these methods, to our knowledge, require using the Microchip products in a manner outside the operating specifications contained in Microchip's Data Sheets. Most likely, the person doing so is engaged in theft of intellectual property.
- Microchip is willing to work with the customer who is concerned about the integrity of their code.

- Neither Microchip nor any other semiconductor manufacturer can guarantee the security of their code. Code protection does not mean that we are guaranteeing the product as "unbreakable."

Code protection is constantly evolving. We at Microchip are committed to continuously improving the code protection features of our products. Attempts to break Microchip's code protection feature may be a violation of the Digital Millennium Copyright Act. If such acts allow unauthorized access to your software or other copyrighted work, you may have a right to sue for relief under that Act.

Legal Notice

Information contained in this publication regarding device applications and the like is provided only for your convenience and may be superseded by updates. It is your responsibility to ensure that your application meets with your specifications. MICROCHIP MAKES NO REPRESENTATIONS OR WARRANTIES OF ANY KIND WHETHER EXPRESS OR IMPLIED, WRITTEN OR ORAL, STATUTORY OR OTHERWISE, RELATED TO THE INFORMATION, INCLUDING BUT NOT LIMITED TO ITS CONDITION, QUALITY, PERFORMANCE, MERCHANTABILITY OR FITNESS FOR PURPOSE. Microchip disclaims all liability arising from this information and its use. Use of Microchip devices in life support and/or safety applications is entirely at the buyer's risk, and the buyer agrees to defend, indemnify and hold harmless Microchip from any and all damages, claims, suits, or expenses resulting from such use. No licenses are conveyed, implicitly or otherwise, under any Microchip intellectual property rights unless otherwise stated.

Trademarks

The Microchip name and logo, the Microchip logo, AnyRate, AVR, AVR logo, AVR Freaks, BitCloud, chipKIT, chipKIT logo, CryptoMemory, CryptoRF, dsPIC, FlashFlex, flexPWR, Heldo, JukeBlox, KeeLoq, Kleer, LANCheck, LINK MD, maXStylus, maXTouch, MediaLB, megaAVR, MOST, MOST logo, MPLAB, OptoLyzer, PIC, picoPower, PICSTART, PIC32 logo, Prochip Designer, QTouch, SAM-BA, SpyNIC, SST, SST Logo, SuperFlash, tinyAVR, UNI/O, and XMEGA are registered trademarks of Microchip Technology Incorporated in the U.S.A. and other countries.

ClockWorks, The Embedded Control Solutions Company, EtherSynch, Hyper Speed Control, HyperLight Load, IntelliMOS, mTouch, Precision Edge, and Quiet-Wire are registered trademarks of Microchip Technology Incorporated in the U.S.A.

Adjacent Key Suppression, AKS, Analog-for-the-Digital Age, Any Capacitor, AnyIn, AnyOut, BodyCom, CodeGuard, CryptoAuthentication, CryptoAutomotive, CryptoCompanion, CryptoController, dsPICDEM, dsPICDEM.net, Dynamic Average Matching, DAM, ECAN, EtherGREEN, In-Circuit Serial Programming, ICSP, INICnet, Inter-Chip Connectivity, JitterBlocker, KleerNet, KleerNet logo, memBrain, Mindi, MiWi, motorBench, MPASM, MPF, MPLAB Certified logo, MPLIB, MPLINK, MultiTRAK, NetDetach, Omniscient Code Generation, PICDEM, PICDEM.net, PICkit, PICtail, PowerSmart, PureSilicon, QMatrix, REAL ICE, Ripple Blocker, SAM-ICE, Serial Quad I/O, SMART-I.S., SQI, SuperSwitcher, SuperSwitcher II, Total Endurance, TSHARC, USBCheck, VariSense, ViewSpan, WiperLock, Wireless DNA, and ZENA are trademarks of Microchip Technology Incorporated in the U.S.A. and other countries.

SQTP is a service mark of Microchip Technology Incorporated in the U.S.A.

Silicon Storage Technology is a registered trademark of Microchip Technology Inc. in other countries.

GestIC is a registered trademark of Microchip Technology Germany II GmbH & Co. KG, a subsidiary of Microchip Technology Inc., in other countries.

All other trademarks mentioned herein are property of their respective companies.

Quality Management System Certified by DNV

ISO/TS 16949

Microchip received ISO/TS-16949:2009 certification for its worldwide headquarters, design and wafer fabrication facilities in Chandler and Tempe, Arizona; Gresham, Oregon and design centers in California and India. The Company's quality system processes and procedures are for its PIC® MCUs and dsPIC® DSCs, KEELOQ® code hopping devices, Serial EEPROMs, microperipherals, nonvolatile memory and analog products. In addition, Microchip's quality system for the design and manufacture of development systems is ISO 9001:2000 certified.

Worldwide Sales and Service

AMERICAS	ASIA/PACIFIC	ASIA/PACIFIC	EUROPE
Corporate Office 2355 West Chandler Blvd. Chandler, AZ 85224-6199 Tel: 480-792-7200 Fax: 480-792-7277 Technical Support: http://www.microchip.com/ support Web Address: www.microchip.com **Atlanta** Duluth, GA Tel: 678-957-9614 Fax: 678-957-1455 **Austin, TX** Tel: 512-257-3370 **Boston** Westborough, MA Tel: 774-760-0087 Fax: 774-760-0088 **Chicago** Itasca, IL Tel: 630-285-0071 Fax: 630-285-0075 **Dallas** Addison, TX Tel: 972-818-7423 Fax: 972-818-2924 **Detroit** Novi, MI Tel: 248-848-4000 **Houston, TX** Tel: 281-894-5983 **Indianapolis** Noblesville, IN Tel: 317-773-8323 Fax: 317-773-5453 Tel: 317-536-2380 **Los Angeles** Mission Viejo, CA Tel: 949-462-9523 Fax: 949-462-9608 Tel: 951-273-7800 **Raleigh, NC** Tel: 919-844-7510 **New York, NY** Tel: 631-435-6000 **San Jose, CA** Tel: 408-735-9110 Tel: 408-436-4270 **Canada - Toronto** Tel: 905-695-1980 Fax: 905-695-2078	**Australia - Sydney** Tel: 61-2-9868-6733 **China - Beijing** Tel: 86-10-8569-7000 **China - Chengdu** Tel: 86-28-8665-5511 **China - Chongqing** Tel: 86-23-8980-9588 **China - Dongguan** Tel: 86-769-8702-9880 **China - Guangzhou** Tel: 86-20-8755-8029 **China - Hangzhou** Tel: 86-571-8792-8115 **China - Hong Kong SAR** Tel: 852-2943-5100 **China - Nanjing** Tel: 86-25-8473-2460 **China - Qingdao** Tel: 86-532-8502-7355 **China - Shanghai** Tel: 86-21-3326-8000 **China - Shenyang** Tel: 86-24-2334-2829 **China - Shenzhen** Tel: 86-755-8864-2200 **China - Suzhou** Tel: 86-186-6233-1526 **China - Wuhan** Tel: 86-27-5980-5300 **China - Xian** Tel: 86-29-8833-7252 **China - Xiamen** Tel: 86-592-2388138 **China - Zhuhai** Tel: 86-756-3210040	**India - Bangalore** Tel: 91-80-3090-4444 **India - New Delhi** Tel: 91-11-4160-8631 **India - Pune** Tel: 91-20-4121-0141 **Japan - Osaka** Tel: 81-6-6152-7160 **Japan - Tokyo** Tel: 81-3-6880- 3770 **Korea - Daegu** Tel: 82-53-744-4301 **Korea - Seoul** Tel: 82-2-554-7200 **Malaysia - Kuala Lumpur** Tel: 60-3-7651-7906 **Malaysia - Penang** Tel: 60-4-227-8870 **Philippines - Manila** Tel: 63-2-634-9065 **Singapore** Tel: 65-6334-8870 **Taiwan - Hsin Chu** Tel: 886-3-577-8366 **Taiwan - Kaohsiung** Tel: 886-7-213-7830 **Taiwan - Taipei** Tel: 886-2-2508-8600 **Thailand - Bangkok** Tel: 66-2-694-1351 **Vietnam - Ho Chi Minh** Tel: 84-28-5448-2100	**Austria - Wels** Tel: 43-7242-2244-39 Fax: 43-7242-2244-393 **Denmark - Copenhagen** Tel: 45-4450-2828 Fax: 45-4485-2829 **Finland - Espoo** Tel: 358-9-4520-820 **France - Paris** Tel: 33-1-69-53-63-20 Fax: 33-1-69-30-90-79 **Germany - Garching** Tel: 49-8931-9700 **Germany - Haan** Tel: 49-2129-3766400 **Germany - Heilbronn** Tel: 49-7131-67-3636 **Germany - Karlsruhe** Tel: 49-721-625370 **Germany - Munich** Tel: 49-89-627-144-0 Fax: 49-89-627-144-44 **Germany - Rosenheim** Tel: 49-8031-354-560 **Israel - Ra'anana** Tel: 972-9-744-7705 **Italy - Milan** Tel: 39-0331-742611 Fax: 39-0331-466781 **Italy - Padova** Tel: 39-049-7625286 **Netherlands - Drunen** Tel: 31-416-690399 Fax: 31-416-690340 **Norway - Trondheim** Tel: 47-7289-7561 **Poland - Warsaw** Tel: 48-22-3325737 **Romania - Bucharest** Tel: 40-21-407-87-50 **Spain - Madrid** Tel: 34-91-708-08-90 Fax: 34-91-708-08-91 **Sweden - Gothenberg** Tel: 46-31-704-60-40 **Sweden - Stockholm** Tel: 46-8-5090-4654 **UK - Wokingham** Tel: 44-118-921-5800 Fax: 44-118-921-5820