AN12121

How to start a development with A71CH

Rev. 1.0 — 22 February 2018
458510

Document information

Info	Content
Keywords	Security IC, IoT, Product support package, TLS, Secure cloud connection, APDU.
Abstract	This document is a short and concise guide describing the existing product support package for designs based on the A71CH solution. It includes references and pointers to the documentation, software tools, source code, development kits and ordering details.

Revision history

Rev	Date	Description
1.0	20180219	First release

Contact information

For more information, please visit: http://www.nxp.com

AN12121   All information provided in this document is subject to legal disclaimers.   © NXP B.V. 2018. All rights reserved.

Application note
COMPANY PUBLIC
Rev. 1.0 — 22 February 2018
458510
2 of 17

1. Introduction

1.1 Scope

This document is the entry point for new designs based on the A71CH security IC. It provides an overview of the existing product support material, as well as where to find it. It is meant to help designers find the correct and appropriate material for each step of the implementation process.

This document provides a brief introduction to A71CH. It describes the reference hardware and development boards. It details the software development environment, source code, software examples, and documentation as well as ordering details.

1.2 Target audience

This document is intended for technical directors, software and hardware engineers who need to get familiar quickly with the existing support package to design secure IoT solutions based on A71CH security IC.

1.3 A71CH overview

The A71CH is a ready-to-use solution enabling ease-of-use security for IoT device makers. It is a secure element capable of securely storing and provisioning credentials, securely connecting IoT devices to public or private clouds and performing cryptographic device authentication.

The A71CH solution provides basic security measures protecting the IC against many physical and logical attacks. It can be integrated in various host platforms and operating systems to secure a broad range of applications. In addition, it is complemented by a comprehensive product support package, offering easy design-in with plug & play host application code, easy-to-use development kits, documentation and IC samples for product evaluation.

2. A71CH development boards

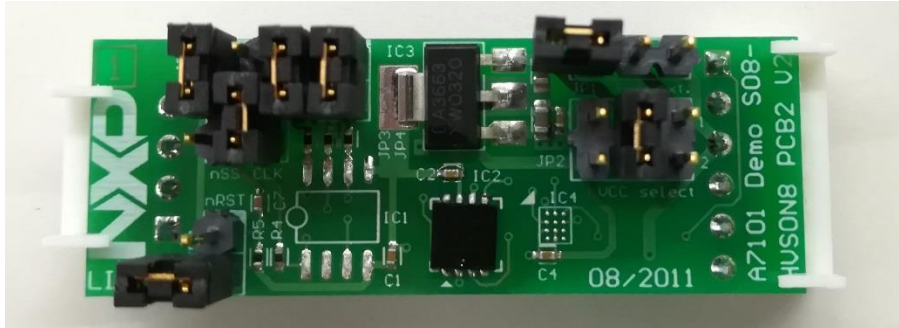A71CH product evaluation is supported by the following development boards:

- A71CH Arduino compatible development kit based on Arduino adaptor board and A71CH Mini PCB board (OM3710/A71CHARD).
- A71CH Mini PCB board (OM3710/A71CHPCB).
- A71CH I^{2}C Bird / Ascot USB adaptor to connect mini PCB to PC (OM37100/B001).

2.1 A71CH Mini PCB board (OM3710/A71CHPCB)

The OM3710/A71CHPCB board is a small PCB containing the A71CH solution and the jumpers for the I^{2}C or SPI host interface selection.

(**Note**: only I^{2}C driver is available; SPI support might be added in future revisions).

The OM3710/A71CHPCB board should be used in combination with OM3710/A71CHARD or OM37100/B001. The Fig 1 illustrates the OM3170/A71CHPCB board.

AN12121

Application note
COMPANY PUBLIC   **Rev. 1.0 — 22 February 2018**
458510   **3 of 17**

(1)   Jumper settings enabling I2C interface of A71CH.

Fig 1.   A71CH mini PCB OM3710/A71CHPCB

The OM71110/A71CHPCB is delivered as part of the OM3710/A71CHARD development kit.

2.2   A71CH Arduino compatible development kit (OM3710/A71CHARD)

The OM3710/A71CHARD is an Arduino development kit containing two items:

- An OM3710/A71CHPCB board
- An Arduino interface board that can be used to connect the A71CH to any host platform featuring an Arduino compatible header (e.g. many LPC, Kinetis and i.MX boards in the market).

In addition, the OM3710/A71CHARD provides dedicated male connectors to plug the OM3710/A71CHPCB to the Arduino interface board without any hardware modification. The Fig 2 shows the Arduino interface board with the OM3710/A71CHPCB board mounted (highlighted in red).

Fig 2.   OM3710/A71CHPCB board mounted into the Arduino interface board

Table 1.   Ordering details for A71CH Arduino development kit

Type number	12NC	Description	Ordering
OM3710/A71CHARD	935368997598	Arduino development kit based on Arduino adaptor board and mini PCB	eCommerce

2.3   USB/I²C bird (OM3710/B001)

The OM3710/B001 board is a complete I²C /USB set enabling to connect a OM3710/A71CHPCB board via USB to a development PC. This kit comes with:
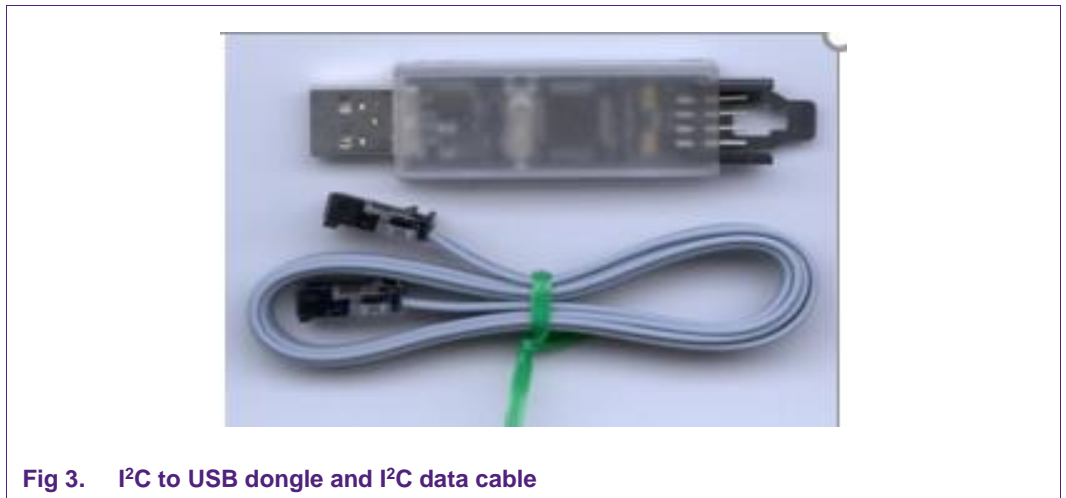
- USB I²C Bird / Ascot adaptor
- An I²C data cable.

Fig 3.   I²C to USB dongle and I²C data cable

To order the OM3710/B001, please contact your NXP representative. It is also possible to execute the A71CH Host Library on a development PC by using the A71CH mini PCB (OM3710/A71CHPCB), the i.MX6UltraLite evaluation kit (MCIMX6UL-EVKB) and the RJCT server.

3.   Supported MCUs / MPUs

The A71CH can be integrated in various host platforms and operating systems. To facilitate fast product evaluation, the A71CH Host software package is ported and ready to be used for the reference host MCUs detailed in this section.

In case that A71CH Host software needs to be ported to another MCU, it is important to note that the A71CH Host interface is based on the Smart Card I2C protocol (SCIIC). This protocol is documented in SCI2C Protocol Specification [SCI2C].

3.1   i.MX6UltraLite evaluation kit (MCIMX6UL-EVKB)

The i.MX6UltraLite processor is a high-performance, ultra-efficient processor family featuring an advanced implementation of a single ARM Cortex-A7 core operating at speeds up to 696 MHz. It is supported by the i.MX6UltraLite evaluation kit (MCIMX6UL-

AN12121

All information provided in this document is subject to legal disclaimers.

© NXP B.V. 2018. All rights reserved.

Application note
COMPANY PUBLIC

Rev. 1.0 — 22 February 2018
458510

5 of 17

EVKB) designed to showcase the most commonly used features of the processor. It facilitates software development through the support of the Linux operating system.

Fig 4.   iMX6ULEVK i.MX6UltraLite evaluation board showing Arduino female connectors

Table 2.   Ordering details for i.MX6UltraLite Evaluation kit

Type number	12NC	Description	Ordering
MCIMX6UL-EVKB	935328353598	Evaluation kit based on i.MX6UltraLite	eCommerce

From a hardware perspective, the i.MX6UltraLite evaluation board can be used in combination with OM3710/A71CHARD with the dedicated Arduino connectors in both PCBs. From a software perspective, it is available a bootable Linux image pre-compiled for i.MX6UltraLite. This software image is ready to be flashed in a microSD memory card and contains the A71CH Host software package already included in it.

The A71CH Quick start guide for OM3710/A71CHARD i.MX6 application note [QUICK_START_IMX6] provides full details about how to get started with the OM3710A71CHARD and i.MX6UltraLite evaluation board. More information about i.MX6UltraLite can be found in [MCIMX6UL_EVKB].

3.2   Kinetis FRDM-K64F

The Kinetis FRDM-K64F development platform is a simple, yet sophisticated design featuring a Kinetis K64 series microcontroller, built on the ARM® Cortex®-M4 core. The FRDM-K64F can be used to evaluate the K64, K63, and K24 Kinetis K series devices. It features the MK64FN1M0VLL12 MCU, which boasts the maximum operation frequency

of 120 MHz, 1 MB of flash, 256 KB RAM, a full-speed USB controller, Ethernet controller, secure digital host controller, and analog and digital peripherals.

The FRDM-K64F hardware is form-factor compatible with the Arduino R3 pin layout, providing a broad range of expansion board options. The onboard interface includes a six-axis digital accelerometer & magnetometer, RGB LED, SDHC, add-on Bluetooth module, add-on RF module, Ethernet and OpenSDAv2, the NXP open-source hardware embedded serial and debug adapter running an open-source bootloader.

Fig 5.   **FRDM-K64F Freedom development platform for Kinetis K64, K63 and K24 MCUs**

Table 3.   **Ordering details for i.MX6UltraLite Evaluation kit**

Type number	12NC	Description	Ordering
FRDM-K64F	935326293598	Freedom development platform for Kinetis K64, K63 and K24 MCUs	eCommerce

From a hardware perspective, the FRDM-K64F evaluation board can be used in combination with OM3710/A71CHARD with the dedicated Arduino connectors. From a software perspective, a MCUXpresso project example is available. This project example contains the A71CH Host software package in it. The project is ready to be imported, built, debugged and executed in Kinetis K64 MCU flash memory using MCUXpresso IDE.

The A71CH Quick start guide for OM3710/A71CHARD for Kinetis K64F application note [QUICK_START_KINETIS] provides full details on how to get started with OM3710A71CHARD and FRDM-K64F evaluation board.

3.3 Kinetis FRDM-KW41Z

The FRDM-KW41Z Freedom development board is a small, low-power, and cost-effective evaluation and development board for application prototyping and demonstration of the KW41Z/31Z/21Z (KW41Z) family of devices. The KW41Z integrates a radio transceiver operating in the 2.36 GHz to 2.48 GHz range (supporting a range of FSK/GFSK and O-QPSK modulations) and an ARM Cortex-M0+ MCU into a single package.

The FRDM-KW41Z development board consists of the KW41Z device with a 32 MHz reference oscillator crystal, RF circuitry (including antenna), 4-Mbit external serial flash, and supporting circuitry in the popular Freedom board form-factor. The board is a

standalone PCB and supports application development with NXP's Bluetooth Low Energy, Generic FSK, and IEEE Std. 802.15.4 protocol stacks including Thread.
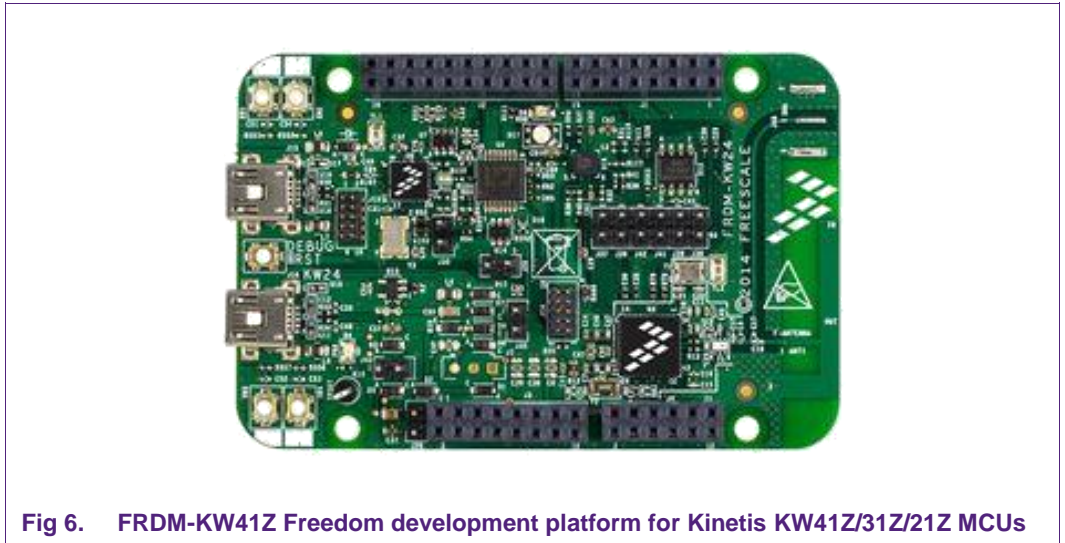

Fig 6.   FRDM-KW41Z Freedom development platform for Kinetis KW41Z/31Z/21Z MCUs

Table 4.   Ordering details for i.MX6UltraLite Evaluation kit

Type number	12NC	Description	Ordering
FRDM-KW41Z	935326317598	FRDM-KW41Z Freedom development platform for Kinetis KW41Z/31Z/21Z MCUs	eCommerce

From a hardware perspective, the FRDM-KW41Z evaluation board can be used in combination with OM3710/A71CHARD with the dedicated Arduino connectors. From a software perspective, a MCUXpresso project example is available. This project example contains the A71CH Host software package in it. The project is ready to be imported, built, debugged and executed in Kinetis KW41Z MCU flash memory using MCUXpresso IDE.

The A71CH Quick start guide for OM3710/A71CHARD for Kinetis KW41Z application note [QUICK_START_KINETIS] provides full details on how get started with OM3710A71CHARD and FRDM-KW41Z evaluation board.

3.4 Kinetis FRDM-K82F

The Freescale Freedom K82 hardware, FRDM-K82F, is a simple yet sophisticated design featuring a Kinetis K series microcontroller built on the ARM® Cortex®-M4 core which features a floating-point unit (FPU).

The FRDM-K82F can be used to evaluate the K80, K81, and K82 Kinetis K series devices. The FRDMK82F board features the K82FN256VLL15 MCU, which boasts a maximum operation frequency of 150 MHz, 256 KB of flash, a 256 KB RAM, a full-speed USB controller with available crystal-less operation, and analog and digital peripherals.
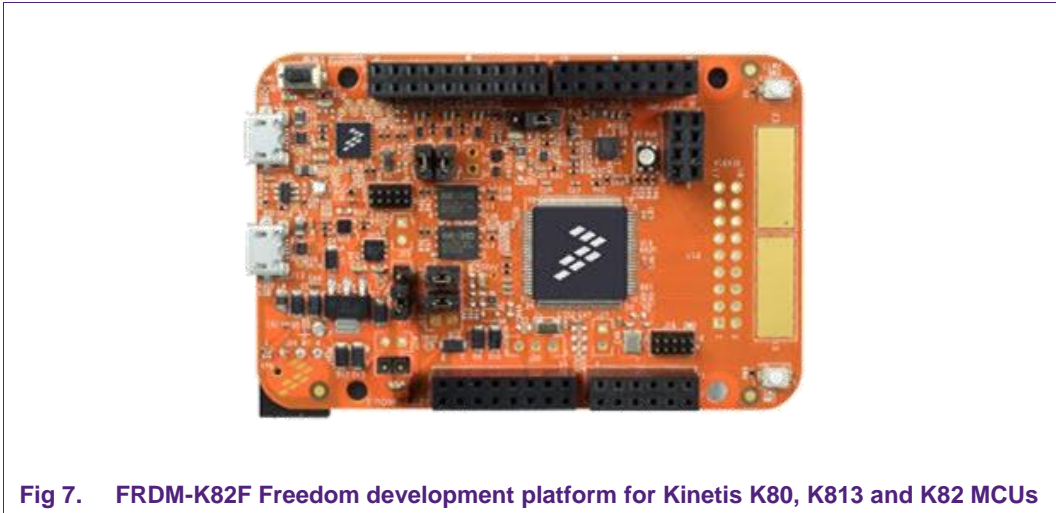
AN12121

Application note
COMPANY PUBLIC

Rev. 1.0 — 22 February 2018
458510

8 of 17

Fig 7. FRDM-K82F Freedom development platform for Kinetis K80, K813 and K82 MCUs

Table 5. Ordering details for i.MX6UltraLite Evaluation kit

Type number	12NC	Description	Ordering
FRDM-K82F	935327211598	Freedom Development Board for Kinetis K80, K81 and K82 MCUs	eCommerce

From a hardware perspective, the FRDM-K82F evaluation board can be used in combination with OM3710/A71CHARD with the dedicated Arduino connectors. From a software perspective, a MCUXpresso project example is available. This project example contains the A71CH Host software package in it. The project is ready to be imported, built, debugged and executed in Kinetis K82F MCU flash memory using MCUXpresso IDE.

The A71CH Quick start guide for OM3710/A71CHARD for Kinetis application note [QUICK_START_KINETIS] provides full details on how get started with OM3710A71CHARD and FRDM-K82F evaluation board.

4. A71CH Host software package contents

The A71CH Host software package is a comprehensive package supporting software development for A71CH-based applications [A71CH_HOST_SW].

The A71CH Host software package includes:

- A71CH Host software support documentation (Doxygen).
- A71CH Host software API source code.
- A71CH Configure tool.
- A71CH API usage examples.
- A71CH OpenSSL engine examples.
- A remote JC Terminal (RJCT) server.

4.1 A71CH Host software support documentation (Doxygen).

The A71CH Host software support documentation is an HTML-based guide that describes in detail all the items included in the A71CH Host software package.

It includes:

- The A71CH Host software API description.
- The A71CH Configuration tool command line options.
- The instructions to run the A71CH API usage and OpenSSL engine examples.
- The instructions to use the RJCT server.

4.2 A71CH Host software API source code

The A71CH Host software API source code are the files written in C language exposing the A71CH interface to a host microcontroller.

4.3 A71CH Configure tool.

The A71CH Configure Tool is a command line tool that supports the insertion of credentials into the A71CH. The command line syntax is documented as part of the A71CH Host software support documentation.

The source code of the A71CH Configure tool is part of the A71CH Host software package.

4.4 A71CH API usage examples

The A71CH API usage examples are pieces of code demonstrating the A71CH Host interface API. These examples demonstrate how to make direct calls to A71CH API for the storage of symmetric keys, the storage of asymmetric keys, for signature generation and verification, for secure channel establishment with the host MCU, share secret key calculation for key agreement (ECDH), and more.

4.5 A71CH OpenSSL Engine examples

The A71CH OpenSSL Engine examples are a set of scripts, which illustrate how to use the standard OpenSSL tools in combination with the A71CH OpenSSL engine to:

- Fetch random numbers from A71CH.
- Create a certificate signing request (CSR) with the private key stored in A71CH.
- Sign a message with a private key stored in A71CH.
- Verify a message with a public key stored in A71CH.
- Set-up a TLS demo for a mutually authenticated and encrypted link between a client and a server system.

4.6 Remote JC Terminal server

The RJCT server is a standalone process that can establish a communication session with a secure element on behalf of a client process. The source code of the RJCT server and the communication module to build clients is included in the A71CH Host software package. The RJCT has the same interface as the NXP CardServer application. The

AN12121

© NXP B.V. 2018. All rights reserved.

Application note
COMPANY PUBLIC

Rev. 1.0 — 22 February 2018
458510

10 of 17

purpose is to provide access to the A71CH over TCP/IP to be able to develop and evaluate applications with the Host software on another platform, e.g. Windows.

5. Application notes documentation

The A71CH security IC comes a set of public application note documents to facilitate the design-in process. This section summarizes the existing documentation.

5.1 AN12119 - Quick start guide for OM3710/A71CHARD and i.MX6UltraLite

This document gives information on how to get started with OM3710A71CHARD development kit and i.MX6UltraLite board. It gives an extensive overview of the hardware and describes the boards configuration options. It also describes the A71CH security IC software architecture and gives step by step instructions to set up the software development environment as well as full directions to run the example application in a Linux platform using the MCIMX6UL-EVKB board [QUICK_START_IMX6].

5.2 AN12134 - Quick start guide for Windows

This document gives information on how to get started with OM3710A71CHPCB development board in a Windows development PC. It gives a detailed overview of the hardware and describes board configuration options. It also describes the A71CH Host software architecture and gives step-by-step instructions to set up the Windows Visual Studio development environment as well as full directions to run the project example in a Windows computer [QUICK_START_WIN].

5.3 AN12135 - Quick start guide for OM3710/A71CHARD and Kinetis

This document gives information on how to get started with OM3710A71CHARD development board and Kinetis boards (FRDM-K64F, FRMD-K82F and FRDM-KW41Z). It gives an extensive overview of the hardware and describes board configuration options. It also describes the A71CH Host software architecture and gives step-by-step instructions to set up the development environment as well as full directions to execute the MCUXpresso project example [QUICK_START_KINETIS].

5.4 AN12133 - A71CH Host software package documentation

This document provides an overview to the A71CH Host software architecture. It details the support documentation and the A71CH Host software directory structure. It also describes the A71CH Configure tool, the Host API usage and OpenSSL engine application examples included as part of the package [AN_A71CH_HOST_SW].

5.5 AN12131 - A71CH for secure connection to AWS cloud

This document describes how the A71CH security IC can be used to establish a secure connection between an IoT device and Amazon Web Services (AWS). It introduces ECC cryptography and SSL/TLS protocol fundamentals and describes step by step the process required for onboarding IoT devices in AWS platform [AWS_CONNECTION].

AN12121

Application note
COMPANY PUBLIC

Rev. 1.0 — 22 February 2018
458510

11 of 17

5.6 AN12132 - A71CH for secure connection to OEM cloud

This document describes how the A71CH security IC can be used to establish a secure connection between an IoT device and the OEM cloud. It introduces ECC cryptography and SSL/TLS protocol fundamentals and for demonstration purposes, it describes step by step how to initiate a TLS/SSL based communication using A71CH OpenSSL Engine example scripts [OEM_CONNECTION].

5.7 AN12120 - A71CH for electronic anti-counterfeit protection

This document describes how A71CH can be used for proof-of-origin verification or anticounterfeit protection. The document introduces ECC cryptography fundamentals, it describes the mechanisms and credentials involved to perform a cryptographic mutual authentication between a server and an IoT device. And finally, for A71CH evaluation and demonstration purposes, it details how a mutual authentication can be performed using the A71CH Configure tool, OpenSSL and A71CH OpenSSL Engine libraries [A71CH_ANTICOUNTERFEIT].

AN12121

Application note
COMPANY PUBLIC

Rev. 1.0 — 22 February 2018
458510

12 of 17

6. Referenced Documents

Table 6. Referenced Documents

[SCI2C]	**SCI2C Protocol Specification** – Revision 1.x only, Docstore an1950**[1]
[QUICK_START_IMX6]	**AN12119 Quick start guide for OM3710A71CHARD i.MX6** – Application note, document number 4582**[1]
[MCIMX6UL_EVKB]	**i.MX6UltraLite Evaluation Kit** - www.nxp.com/iMX6ULEVK
[A71CH_HOST_SW]	**A71CH Host Software Package (Windows Installer) –** DocStore, document number sw4673xx[1], Version 01.03.00 (or later), available on www.nxp.com/A71CH **A71CH Host Software Package (Bash installer) –** DocStore, document number sw4672xx[1], Version 01.03.00 (or later), available on www.nxp.com/A71CH
[A71CH_APDU]	**APDU Specification of A71CH Security Module -** DocStore ds4094**[1]
[AN_A71CH_HOST_SW]	**AN12133 A71CH Host software package documentation** – Application note, document number 4643**[1]
[OEM_CONNECTION]	**AN12132 A71CH for secure Connection to OEM Cloud** – Application note, document number 4642**[1]
[AWS_CONNECTION]	**AN12131 A71CH for secure Connection to OEM** Cloud – Application note, document number 4641**[1]
[A71CH_ANTICOUNTERFEIT]	**AN12120 A71CH for electronic anti-counterfeit** – Application note, document number 4583**[1]
[A71CH_OPENSSL_ENGINE]	**A71CH OpenSSL Engine** – DocStore, document number um4334**[1]
[QUICK_START_WIN]	**AN12134 Quick start guide for Windows** – Application note, document number 4644**[1]
[QUICK_START_KINETIS]	**AN12135 Quick start guide for OM3710A71CHARD and Kinetis** – Application note, document number 4645**[1]

[1] **… document version number

AN12121

Application note
COMPANY PUBLIC

All information provided in this document is subject to legal disclaimers.

Rev. 1.0 — 22 February 2018
458510

© NXP B.V. 2018. All rights reserved.

13 of 17

7. Legal information

7.1 Definitions

Draft — The document is a draft version only. The content is still under internal review and subject to formal approval, which may result in modifications or additions. NXP Semiconductors does not give any representations or warranties as to the accuracy or completeness of information included herein and shall have no liability for the consequences of use of such information.

7.2 Disclaimers

Limited warranty and liability — Information in this document is believed to be accurate and reliable. However, NXP Semiconductors does not give any representations or warranties, expressed or implied, as to the accuracy or completeness of such information and shall have no liability for the consequences of use of such information. NXP Semiconductors takes no responsibility for the content in this document if provided by an information source outside of NXP Semiconductors.

In no event shall NXP Semiconductors be liable for any indirect, incidental, punitive, special or consequential damages (including - without limitation - lost profits, lost savings, business interruption, costs related to the removal or replacement of any products or rework charges) whether or not such damages are based on tort (including negligence), warranty, breach of contract or any other legal theory.

Notwithstanding any damages that customer might incur for any reason whatsoever, NXP Semiconductors' aggregate and cumulative liability towards customer for the products described herein shall be limited in accordance with the *Terms and conditions of commercial sale* of NXP Semiconductors.

Right to make changes — NXP Semiconductors reserves the right to make changes to information published in this document, including without limitation specifications and product descriptions, at any time and without notice. This document supersedes and replaces all information supplied prior to the publication hereof.

Suitability for use — NXP Semiconductors products are not designed, authorized or warranted to be suitable for use in life support, life-critical or safety-critical systems or equipment, nor in applications where failure or malfunction of an NXP Semiconductors product can reasonably be expected to result in personal injury, death or severe property or environmental damage. NXP Semiconductors and its suppliers accept no liability for inclusion and/or use of NXP Semiconductors products in such equipment or applications and therefore such inclusion and/or use is at the customer's own risk.

Applications — Applications that are described herein for any of these products are for illustrative purposes only. NXP Semiconductors makes no representation or warranty that such applications will be suitable for the specified use without further testing or modification.

Customers are responsible for the design and operation of their applications and products using NXP Semiconductors products, and NXP Semiconductors accepts no liability for any assistance with applications or customer product design. It is customer's sole responsibility to determine whether the NXP Semiconductors product is suitable and fit for the customer's applications and products planned, as well as for the planned application and use of customer's third party customer(s). Customers should provide appropriate design and operating safeguards to minimize the risks associated with their applications and products.

NXP Semiconductors does not accept any liability related to any default, damage, costs or problem which is based on any weakness or default in the customer's applications or products, or the application or use by customer's third party customer(s). Customer is responsible for doing all necessary testing for the customer's applications and products using NXP Semiconductors products in order to avoid a default of the applications and the products or of the application or use by customer's third party customer(s). NXP does not accept any liability in this respect.

Export control — This document as well as the item(s) described herein may be subject to export control regulations. Export might require a prior authorization from competent authorities.

Translations — A non-English (translated) version of a document is for reference only. The English version shall prevail in case of any discrepancy between the translated and English versions.

Evaluation products — This product is provided on an "as is" and "with all faults" basis for evaluation purposes only. NXP Semiconductors, its affiliates and their suppliers expressly disclaim all warranties, whether express, implied or statutory, including but not limited to the implied warranties of non-infringement, merchantability and fitness for a particular purpose. The entire risk as to the quality, or arising out of the use or performance, of this product remains with customer.

In no event shall NXP Semiconductors, its affiliates or their suppliers be liable to customer for any special, indirect, consequential, punitive or incidental damages (including without limitation damages for loss of business, business interruption, loss of use, loss of data or information, and the like) arising out the use of or inability to use the product, whether or not based on tort (including negligence), strict liability, breach of contract, breach of warranty or any other theory, even if advised of the possibility of such damages.

Notwithstanding any damages that customer might incur for any reason whatsoever (including without limitation, all damages referenced above and all direct or general damages), the entire liability of NXP Semiconductors, its affiliates and their suppliers and customer's exclusive remedy for all of the foregoing shall be limited to actual damages incurred by customer based on reasonable reliance up to the greater of the amount actually paid by customer for the product or five dollars (US$5.00). The foregoing limitations, exclusions and disclaimers shall apply to the maximum extent permitted by applicable law, even if any remedy fails of its essential purpose.

7.1 Licenses

ICs with DPA Countermeasures functionality

NXP ICs containing functionality implementing countermeasures to Differential Power Analysis and Simple Power Analysis are produced and sold under applicable license from Cryptography Research, Inc.

7.2 Trademarks

Notice: All referenced brands, product names, service names and trademarks are property of their respective owners.

FabKey — is a trademark of NXP B.V.

I²C-bus — logo is a trademark of NXP B.V.

8. List of figures

9. List of tables

10. Contents

Mouser Electronics

Authorized Distributor

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

[NXP](#):
  [OM3710/A71CHARD](#)