



Arm® CryptoCell™-713

Product revision: r0p0-00rel0

OSS RT Release Note

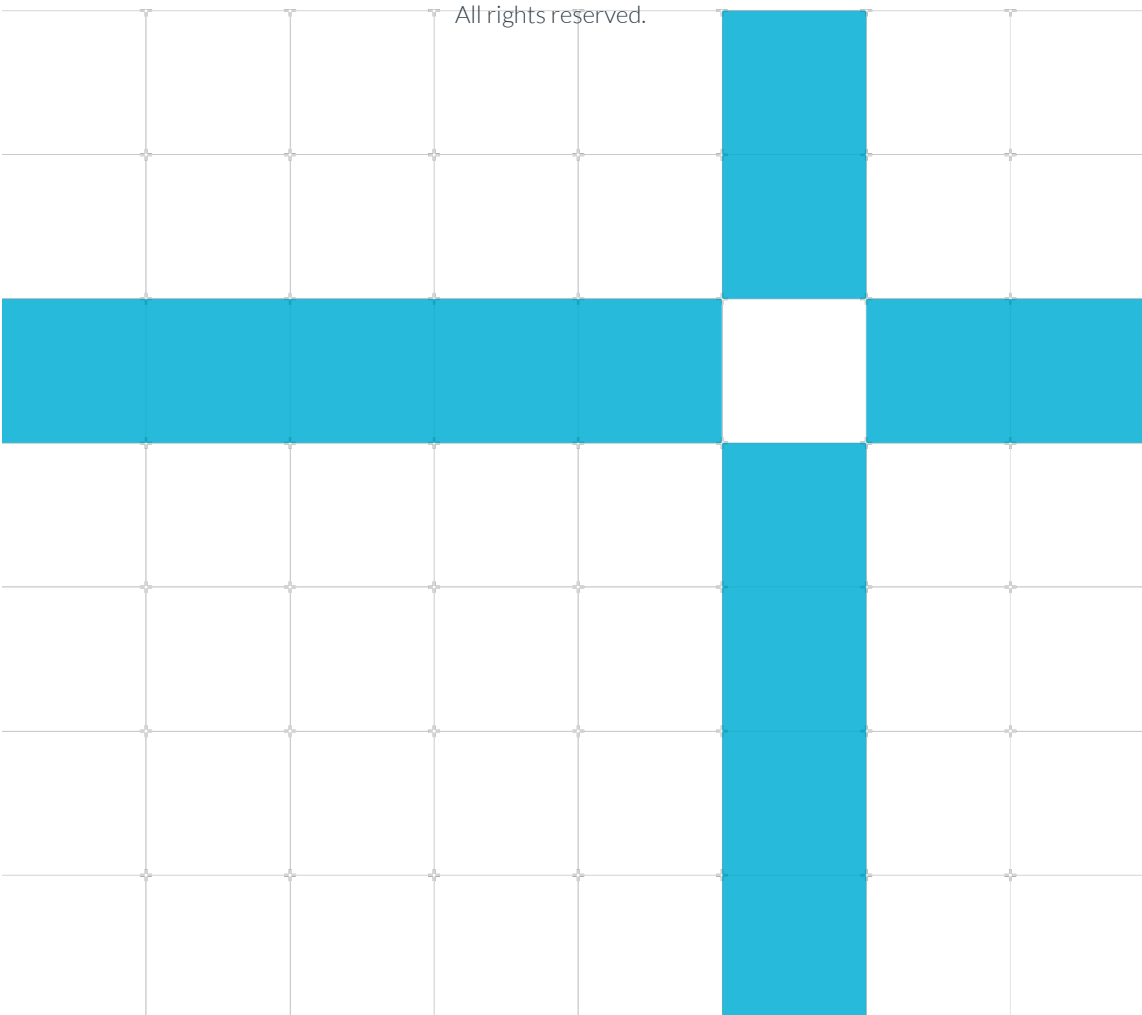
Non-Confidential

Copyright © 2020 Arm Limited (or its affiliates).

All rights reserved.

PJDOC-

1779577084-32286



Arm® CryptoCell™-713 OSS RT Release Note

Copyright © 2020 Arm Limited (or its affiliates). All rights reserved.

Non-Confidential Proprietary Notice

This document is protected by copyright and other related rights and the practice or implementation of the information contained in this document may be protected by one or more patents or pending patent applications. No part of this document may be reproduced in any form by any means without the express prior written permission of Arm. No license, express or implied, by estoppel or otherwise to any intellectual property rights is granted by this document unless specifically stated.

Your access to the information in this document is conditional upon your acceptance that you will not use or permit others to use the information for the purposes of determining whether implementations infringe any third party patents.

THIS DOCUMENT IS PROVIDED "AS IS". ARM PROVIDES NO REPRESENTATIONS AND NO WARRANTIES, EXPRESS, IMPLIED OR STATUTORY, INCLUDING, WITHOUT LIMITATION, THE IMPLIED WARRANTIES OF MERCHANTABILITY, SATISFACTORY QUALITY, NON-INFRINGEMENT OR FITNESS FOR A PARTICULAR PURPOSE WITH RESPECT TO THE DOCUMENT. For the avoidance of doubt, Arm makes no representation with respect to, and has undertaken no analysis to identify or understand the scope and content of, patents, copyrights, trade secrets, or other rights.

This document may include technical inaccuracies or typographical errors.

TO THE EXTENT NOT PROHIBITED BY LAW, IN NO EVENT WILL ARM BE LIABLE FOR ANY DAMAGES, INCLUDING WITHOUT LIMITATION ANY DIRECT, INDIRECT, SPECIAL, INCIDENTAL, PUNITIVE, OR CONSEQUENTIAL DAMAGES, HOWEVER CAUSED AND REGARDLESS OF THE THEORY OF LIABILITY, ARISING OUT OF ANY USE OF THIS DOCUMENT, EVEN IF ARM HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

This document consists solely of commercial items. You shall be responsible for ensuring that any use, duplication or disclosure of this document complies fully with any relevant export laws and regulations to assure that this document or any portion thereof is not exported, directly or indirectly, in violation of such export laws. Use of the word "partner" in reference to Arm's customers is not intended to create or refer to any partnership relationship with any other company. Arm may make changes to this document at any time and without notice.

If any of the provisions contained in these terms conflict with any of the provisions of any click through or signed written agreement covering this document with Arm, then the click through or signed written agreement prevails over and supersedes the conflicting provisions of these terms. This document may be translated into other languages for convenience, and you agree that if there is any conflict between the English version of this document and any translation, the terms of the English version of the Agreement shall prevail.

The Arm corporate logo and words marked with ® or ™ are registered trademarks or trademarks of Arm Limited (or its affiliates) in the US and/or elsewhere. All rights reserved. Other brands and names mentioned in this document may be the trademarks of their respective owners. Please follow Arm's trademark usage guidelines at <http://www.arm.com/company/policies/trademarks>.

Copyright © 2020 Arm Limited (or its affiliates). All rights reserved.

Arm Limited. Company 02557590 registered in England.

110 Fulbourn Road, Cambridge, England CB1 9NJ.

(LES-PRE-20349)

Confidentiality Status

This document is Non-Confidential. The right to use, copy and disclose this document may be subject to license restrictions in accordance with the terms of the agreement entered into by Arm and the party that Arm delivered this document to.

Unrestricted Access is an Arm internal classification.

Product status

The information in this document is Final, that is for a developed product.

Web address

www.arm.com

Contents

1 Conventions	5
1.1 Glossary	5
1.2 Typographical conventions.....	5
2 Release overview.....	7
2.1 Product description.....	7
2.2 Release status.....	7
2.3 Standards compliance.....	7
3 Release contents.....	12
3.1 Deliverables	12
3.1.1 Associated products	12
3.2 Differences from previous release.....	12
3.3 Known limitations	13
4 Get started	14
4.1 Licensing information	14
4.2 Download the product.....	14
4.2.1 Unpack the product	14
4.2.2 Compile the product.....	15
4.2.3 Directory structure.....	16
4.3 Adapt the product for your system.....	18
4.4 Examples	18
5 Support	19
5.1 Tools.....	19
5.2 OS	19

1 Conventions




The following subsections describe conventions used in Arm documents.




1.1 Glossary

The Arm Glossary is a list of terms used in Arm documentation, together with definitions for those terms. The Arm Glossary does not contain terms that are industry standard unless the Arm meaning differs from the generally accepted meaning.

See the Arm Glossary for more information: <https://developer.arm.com/glossary>.

1.2 Typographical conventions

Convention	Use
<i>italic</i>	Introduces citations.
bold	Highlights interface elements, such as menu names. Denotes signal names. Also used for terms in descriptive lists, where appropriate.
<code>monospace</code>	Denotes text that you can enter at the keyboard, such as commands, file and program names, and source code.
<code>monospace bold</code>	Denotes language keywords when used outside example code.
<code>monospace <u>underline</u></code>	Denotes a permitted abbreviation for a command or option. You can enter the underlined text instead of the full command or option name.
<and>	Encloses replaceable terms for assembler syntax where they appear in code or code fragments. For example: <pre>MRC p15, 0, <Rd>, <CRn>, <CRm>, <Opcode_2></pre>
small CAPITALS	Used in body text for a few terms that have specific technical meanings, that are defined in the Arm® Glossary. For example, implementation defined, implementation specific, unknown, and unpredictable.
 Caution	This represents a recommendation which, if not followed, might lead to system failure or damage.
 Warning	This represents a requirement for the system that, if not followed, might result in system failure or damage.
 Danger	This represents a requirement for the system that, if not followed, will result in system failure or damage.

 Note	This represents an important piece of information that needs your attention.
 Tip	This represents a useful tip that might make it easier, better, or faster to perform a task.
 Remember	This is a reminder of something important that relates to the information you are reading.

2 Release overview

2.1 Product description

The Arm® CryptoCell™-713 is an embedded security platform for high-performance systems. It is aimed primarily at client devices, such as smartphones, tablets, smart TVs, and set-top boxes. It offers a rich set of cryptographic services, targeting multiple threats.

2.2 Release status

This is the REL release of r0p0 Arm® CryptoCell™-713 software.

These deliverables are being released under the terms of the agreement between Arm and each licensee (the “Agreement”). All planned verification and validation is complete.

The release is suitable for volume production under the terms of the Agreement.

2.3 Standards compliance

CryptoCell-713 complies with the following specifications:

Table 2-1 CryptoCell-713 compliance

Document ID	Document name	Compliance
IHI 0022F	AMBA® AXI and ACE Protocol Specification, December 2017	Full
DEN 0083	Arm® Platform Security Architecture Trusted Base System Architecture for Arm®v6-M, Arm®v7-M and Arm®v8-M	Compliant, excluding the Non-Volatile counters R010_TBSA_COUNT and R020_TBSA_COUNT.
DEN 0022D	Arm® Power State Coordination Interface Platform Design Document	Full
IHI 0024C	AMBA® APB Protocol Specification, April 2010	Full
IHI 0068C	AMBA® Low Power Interface Specification, September 2016	Full
DEN 0006D	Arm® Trusted Board Boot Requirements CLIENT (TBBR- CLIENT) Armv8-A	Full
ANSI X3.92-1981	Data Encryption Algorithm	Full
ANSI X3.106-1983	Data Encryption Algorithm – Modes of Operation	Compliant with ECB, CBC for CryptoCell REE host.
ANSI X9.42-2003	Public Key Cryptography for the Financial Services Industry: Agreement of Symmetric Keys Using Discrete Logarithm Cryptography, 2003	Compliant with sections 7.1, 7.2, 7.3, 7.4, 7.5.1, 7.7.1, 7.7.2, 8.1.1, 8.1.2, 8.1.3, 8.1.4, and Annex B.

Document ID	Document name	Compliance
ANSI X9.52-1998	<i>Triple Data Encryption Algorithm Modes of Operation</i>	Compliant with ECB and CBC for CryptoCell REE host.
ANSI X9.62-2005	<i>Public Key Cryptography for the Financial Services Industry, The Elliptic Curve Digital Signature Algorithm (ECDSA), 2005</i>	Compliant with sections 7.2, 7.3, and 7.4.1 – prime curves.
ANSI X9.63-2011	<i>Public Key Cryptography for the Financial Services Industry – Key Agreement and Key Transport Using Elliptic Curve Cryptography, 2011</i>	Compliant with sections 5.2, 5.3, 5.4.1, 5.6.2, 5.6.3, 5.7 (MAC and HMAC), 5.9, 6.1, 6.2, 6.3, 6.4, 6.5, and 6.6.
BSI AIS-31	<i>Functionality Classes and Evaluation Methodology for True Random Number Generators, version 3.1, September 2001</i>	Compliant in an implementation using FETRNG driver.
FIPS Publication 140-2	<i>Security Requirements for Cryptographic Modules, December 3, 2002C</i>	Ready for certification
FIPS Publication 180-4	<i>Secure Hash Standard (SHS), December 3, 2002C</i>	Compliant, excluding support for truncated hash operation.
FIPS Publication 186-4	<i>Digital Signature Standard (DSS), July 2013</i>	Compliant with sections 5.1, 6.2, 6.3, 6.4, B.1.2, B.2.2, B.3.6, B.4.2, C.3.1, C.3.3, C.3.5, C.9, and D.1.2.
FIPS Publication 197	<i>Advanced Encryption Standard</i>	Full
FIPS Publication 198-1	<i>The Keyed-Hash Message Authentication Code (HMAC), July 2008</i>	Full
ISO/IEC 9797-1	<i>Message Authentication Codes (MACs) -- Part 1: Mechanisms using a block cipher, July 2008</i>	Compliant with CBC-MAC without padding, output transformation based on sections 6.2, 6.3.1, 6.4, 6.5.1, and 7.1.
IEEE 802.15.4	<i>IEEE Standard for Local and metropolitan area networks—Part 15.4: Low-Rate Wireless Personal Area Networks (LR-WPANs), September 2011</i>	Compliant with CCM* (Annex B).
IEEE 1363-2000	<i>IEEE Standard for Standard Specifications for Public-Key Cryptography, 2000</i>	Compliant with sections 7.2.1, 8 (excluding 8.2.6, 8.2.7, 8.2.8, 8.2.9), 10.3, 11, 12.2, 13
ISO/IEC 18033-2:2006	<i>Information technology -- Security techniques -- Encryption algorithms -- Part 2: Asymmetric ciphers, May 2006</i>	Compliant with sections 10.2, 10.2.1, 10.2.3, and 10.2.4.
NIST SP 800-22	<i>A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications, April 2010</i>	The second phase in the CryptoCell-713 TRNG characterization process is compliant with this standard.
NIST SP 800-38A	<i>Recommendation for Block Cipher Modes of Operation: Methods and Techniques</i>	Compliant with sections 6.1, 6.2, 6.4, and 6.5.
NIST SP 800-38A Addendum	<i>Recommendation for Block Cipher Modes of Operation: Three Variants of Ciphertext Stealing for CBC Mode</i>	Compliant with CBC-CTS3.
NIST SP 800-38B	<i>NIST SP 800-38B</i>	Full

Document ID	Document name	Compliance
NIST SP 800-38C, July 2007	<i>Recommendation for Block Cipher Modes of Operation: the CCM Mode for Authentication and Confidentiality</i>	Full
NIST SP 800-38D, November 2007	<i>Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC</i>	Full
NIST SP 800-38E	<i>Recommendation for Block Cipher Modes of Operation: the XTSAES Mode for Confidentiality on Storage Devices</i>	Not supported for Trusted environments.
NIST SP 800-38F	<i>Recommendation for Block Cipher Modes of Operation: Methods for Key Wrapping</i>	Full
NIST SP 800-56A	<i>Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography Rev. 2, May 2013</i>	Compliant with sections 5.1, 5.2, 5.3, 5.4, 5.5.1.1, 5.6.1, 5.6.2.3, 5.7.1.1, 5.7.1.2, and 5.8.2.
NIST SP 800-56B	<i>Recommendation for Pair-Wise Key Establishment Schemes Using Integer Factorization Cryptography</i>	Section 7.23 based on AES wrap.
NIST SP 800-67	<i>Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher Rev. 1</i>	Full
NIST SP 800-90A	<i>Recommendation for Random Number Generation Using Deterministic Random Bit Generators, January 2012</i>	Compliant with section 10.2 – DRBG mechanism based on block ciphers.
NIST SP 800-90B	<i>Recommendation for the Entropy Sources Used for Random Bit Generation, January 2018</i>	Compliant with sections 3.14, 4.4, and 5.
NIST SP 800-90C	<i>Recommendation for Random Bit Generator (RBG) Constructions, April 2016</i>	Full
NIST SP 800-108	<i>Recommendation for Key Derivation Using Pseudorandom Functions</i>	Compliant with section 5.1.
NIST SP 800-135	<i>Recommendation for Key Derivation Using Pseudorandom Functions, December 2011</i>	Compliant with section 4.1. Support in other sections for the cryptographic operations, but the full protocol is not supported.
PKCS #1 v1.5	<i>Public-Key Cryptography Standards RSA Encryption, November 1993</i>	Compliant with backward compatibility required by PKCS#1 Version 2.1.
PKCS #1 v2.1	<i>Public-Key Cryptography Standards RSA Cryptography Specifications, June 2002</i>	Compliant, excluding ASN.1 syntax.
PKCS #3	<i>Public-Key Cryptography Standards Diffie Hellman Key Agreement Standard</i>	Full
PKCS #7 v1	<i>Public-Key Cryptography Standards Cryptographic Message Syntax Standard, November 1993</i>	Compliant with section 10.3.
RFC 2104	<i>HMAC: Keyed-Hashing for Message Authentication, February 1997</i>	Compliant with SHA1.
RFC 3394	<i>Advanced Encryption Standard (AES) Key Wrap Algorithm, September 2002</i>	Compliant excluding support for truncation to 96 bits.

Document ID	Document name	Compliance
RFC 3566	<i>The AES-XCBC-MAC-96 Algorithm and Its Use with IPsec</i> , September 2002	Compliant excluding support for truncation to 96 bits.
RFC 3686	<i>Using Advanced Encryption Standard (AES) Counter Mode With IPsec Encapsulating Security Payload (ESP)</i> , January 2004	Compliant only for Trusted environment.
RFC 4106	<i>The Use of Galois/Counter Mode (GCM) in IPsec Encapsulating Security Payload (ESP)</i> , June 2005	Full
RFC 4309	<i>Using Advanced Encryption Standard (AES) CCM Mode with IPsec Encapsulating Security Payload (ESP)</i> , December 2005	Full
RFC 4543	<i>The Use of Galois Message Authentication Code (GMAC) in IPsec ESP and AH</i> , May 2006	Full
RFC 5280	<i>Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile</i> , May 2008	Compliant with section 4 – Secure Boot certificates and Secure Debug certificates.
RFC 5869	<i>HMAC-based Extract-and-Expand Key Derivation Function (HKDF)</i> , May 2010	Full
SEC 2 v1	<i>Recommended Elliptic Curve Domain Parameters</i> , September 20, 2000	Compliant with section 2, 160-bit domains. Smaller domains are not supported.
SEC 2 v2	<i>Recommended Elliptic Curve Domain Parameters</i> , January 27, 2010	Compliant with section 2.
SM2	<i>Public Key Cryptographic Algorithm Based on Elliptic Curves</i> (December 2010)	Full
GM/T 0009-2012	<i>SM2 Cryptography Algorithm Application Specification</i>	Full
GB/T 0003.1-2012	<i>Public Key Cryptographic Algorithm SM2 Based on Elliptic Curves - Part 1: General</i>	Full
GB/T 0003.2-2012	<i>Public Key Cryptographic Algorithm SM2 Based on Elliptic Curves - Part 2: Digital Signature Algorithm</i>	Full
GB/T 0003.3-2012	<i>Public Key Cryptographic Algorithm SM2 Based on Elliptic Curves - Part 3: Key Exchange Protocol</i>	Full
GB/T 0003.4-2012	<i>Public Key Cryptographic Algorithm SM2 Based on Elliptic Curves - Part 4: Public Key Encryption Algorithm</i>	Full
GB/T 0003.5-2012	<i>Public Key Cryptographic Algorithm SM2 Based on Elliptic Curves - Part 5: Parameter Definition</i>	Full
GM/T 0010-2012	<i>SM2 Cryptography Message Syntax Specification</i>	Full
GM/T 0004-2012	<i>SM3 Cryptographic Hash Algorithm</i> (December 2012)	Full

Document ID	Document name	Compliance
GM/T 0002-2012	<i>SM4 Block Cipher Algorithm</i>	Full
GB/T 17964-2008	<i>Information Technology - Security Techniques - Modes of Operation for a Block Cipher</i>	Full
SECG SEC1	<i>Elliptic Curve Cryptography, 2000</i>	Compliant with sections 2.1.1, 2.2.1, 3.1.1,
JESD223C	<i>Universal Flash Storage Host Controller Interface (UFSHCI), Version 2.1, 2000</i>	Compliant with sections 6.3.4 and 9.4 (ESSIV), and sections 9.2 (no elephant diffuser) and 6.3.2 (BitLocker).

3 Release contents

The following subsections describe:

- The component parts that are delivered as part of this release.
- Any changes since the previous release.
- Any known issues and limitations exist at the time of this release.

3.1 Deliverables

Arm® CryptoCell-713 OSS includes the following deliverables:

- CryptoCell-713 runtime software.
- CryptoCell-713 runtime software integration tests.
- CryptoCell-713 runtime tools.
- Runtime API documentation: Arm® CryptoCell-713 Runtime Software Developers Manual.



Note

Documentation may change between product releases. For the latest documentation bundle, please check the delivery platform.

3.1.1 Associated products

The following parts are available to licensees only:

- Arm® CryptoCell-713 Boot Services
- Arm® CryptoCell-713 Hardware

3.2 Differences from previous release

This is the first release of CryptoCell-713 runtime software OSS.

Known limitations

The following table describes any issues known at the time of this release.

Table 3-1 Defects and missing functionality in this release

Issue	Component	Description
RN-008-CC006-ROPO-00RELO	Non-confidential TEE Runtime SW Integration Test Package	Key derivation standard modes, commented in <code>cc_kdf.c</code> , are not up to date.



The ID is for reference only.

4 Get started

This section describes how to get you started with accessing, setting up, and using Arm® CryptoCell™-713.

4.1 Licensing information

The Arm® CryptoCell-713 runtime library and integration tests are published under two optional licenses, located at the root of the project tree:

- BSD-3 clause - Full license is disclosed in `BSD-3-Clause.txt`.
- Arm non-OSI - Full license is disclosed in `Arm-proprietary-license.txt`.

4.2 Download the product

Arm delivers the files through github.

You can download the product package in one of the following ways:

- Download a `.zip` file directly from <https://github.com/ARM-software/cryptocell-713-runtime>
- Use one of the following git clone commands:



The target directory is only mentioned to align with the compilation commands listed afterwards.

-
- o `git clone https://github.com/ARM-software/cryptocell-713-runtime.git cryptocell-rt`
 - o `git clone git@github.com:ARM-software/cryptocell-713-runtime.git cryptocell-rt`

You can download the product package as a single zip file: `cryptocell-713-runtime-master.zip`.

4.2.1 Unpack the product

If you downloaded a `.zip` file directly from github, perform the following steps to unpack the product package:

1. Relocate the package file:
Copy the `.zip` files to the directory where these files are to be installed.
2. Unzip the package.
This command extracts the package into a directory with the same name as the package name.

4.2.2 Compile the product

The following steps describe how to compile this product.

3. Set the environment variables.

A typical setup is as follows:

```
export ARCH=arm64
export CROSS_COMPILE=<compiler-prefix>
export COMPILER_TYPE=gcc
export PATH=$PATH:/path/to/compiler/executable/dir/bin
export TEE_OS=linux64
export KERNEL_DIR=/path/to/kernel/
export TEST_BOARD=<your-board_name> (either juno or zynq)
export TEST_AL_CONFIG_NUM=< Test configuration index >
```

Where the test configuration index depends on your test board, use the appropriate configuration number, as specified in Table 4-1:

Table 4-1 Test board

Test board (TEST_BOARD)	Configuration number (TEST_AL_CONFIG_NUM)
juno	10
Zynq	3

4. It is assumed that the current location includes the extracted directory Cryptocell-713-TEE-Lib-master:

```
% cd Cryptocell-713-TEE-Lib-master
% make -C host/src ARCH=arm64 COMPILER_TYPE=gcc TEE_OS=linux64
```

The Non-Confidential TEE library is located in `host/lib`.

5. Execute the following commands to build the corresponding Non-Confidential TEE runtime SW Integration tests:

```
% make -C host/src/tests/test_engine ARCH=arm64 COMPILER_TYPE=gcc
TEE_OS=linux64 TEST_BOARD=juno TEST_AL_CONFIG_NUM=10
% make -C host/src/tests/integration* ARCH=arm64 COMPILER_TYPE=gcc
TEE_OS=linux64 TEST_BOARD=juno TEST_AL_CONFIG_NUM=10
```

The integration test executables can be found in `host/bin`, which need to be tested in the hardware under test.

6. Compile the Non-Confidential TEE runtime SW utilities:

Before compiling the runtime utilities, we recommend:

- a. Retrieving OpenSSL 1.0.2g
- b. Placing it in `./utils/src/openssl` and building it first.

The following commands are an example of how to achieve this task:

```
% cd utils/src/
% CROSS_COMPILEsrc=$CROSS_COMPILE
```

```
% unset CROSS_COMPILE
% wget https://www.openssl.org/source/openssl-1.0.2g.tar.gz
% tar xf openssl-1.0.2g.tar.gz
% cd openssl-1.0.2g
% ./Configure shared linux-x86_64
% make
% make test
% cd .. # back to ./utils/src
% ln -s openssl-1.0.2g openssl
% make
% export CROSS_COMPILE=$CROSS_COMPILEsrc
```

The utilities executables can be found in `utils/bin`.

4.2.3 Directory structure

Figure 4-1 and shows the principal directory structure of this release created after unpacking the bundle:

Figure 4-1 CryptoCell-713 TEE Runtime SW , Integration Test and utilities directory structure

```
Cryptocell-713-TEE-Lib-master/
|-- codesafe
|   |-- src
|       |-- crypto_api
|           |-- cc7x_sym
|               |-- adaptor
|                   |-- api
|                       |-- driver
|                           |-- chinese_cert
|                               |-- common
|                                   |-- dh
|                                       |-- ec_wrst
|                                           |-- ecc_domains
|                                               |-- fips
|                                                   |-- kdf
|                                                       |-- pki
|                                                           |-- common
|                                                               |-- ec_wrst
|                                                                   |-- rsa
|                                                                       |-- rnd_dma
|                                                                           |-- local
|                                                                               |-- rsa
|                                                                                   |-- sm2
|                                                                                       |-- auxiliary
|                                                                                           |-- dsa
|                                                                                               |-- internal
|                                                                                                   |-- ke
|                                                                                                       |-- secure_boot_debug
|                                                                                                           |-- bsv_rsa_driver
|                                                                                                               |-- cc7x
|                                                                                                                   |-- cert_parser
|                                                                                                                       |-- prop
|                                                                                                                           |-- x509
|                                                                                                         |-- platform
|                                                                                                             |-- hal
```



```
|      |      |      |-- cc7x
|      |      |      |-- pal
|      |      |      |-- stage
|      |      |      |-- rt
|      |      |      |-- cc7x
|      |      |-- secure_boot
|      |      |-- prop
|      |      |-- x509
|      |-- secure_debug
|-- doxygen
|  |-- additional_doc_files_cc713
|-- doxygen-it
|  |-- additional_doc_files_cc713_it
|-- host
|  |-- src
|  |  |-- cc7x_sbromlib
|  |  |-- cc7x_teelib
|  |  |-- full
|  |  |-- hal
|  |  |-- cc7x_tee
|  |  |-- pal
|  |  |  |-- cc_linux
|  |  |  |-- linux64
|  |  |  |-- driver
|  |  |-- tests
|  |  |  |-- TestAL
|  |  |  |  |-- configs
|  |  |  |  |-- hal
|  |  |  |  |  |-- Juno
|  |  |  |  |  |-- Zynq
|  |  |  |  |  |-- include
|  |  |  |  |-- pal
|  |  |  |  |  |-- include
|  |  |  |  |  |-- linux
|  |  |  |-- integration_cc7x3
|  |  |  |  |-- cc71x_tee
|  |  |  |  |-- cc71x_tee_ree
|  |  |-- proj
|  |  |  |-- cc7x
|  |  |-- test_engine
|  |  |-- tests_helper
|  |  |-- menu_engine
|  |-- utils
|-- shared
|  |-- hw
|  |  |-- ree_include
|  |  |-- tee_include
|  |-- include
|  |  |-- boot
|  |  |  |-- cc7x_tee
|  |  |-- cc_util
|  |  |-- crypto_api
|  |  |  |-- cc7x_tee
|  |  |-- pal
|  |  |  |-- cc_linux
|  |  |  |-- linux64
|  |  |-- proj
|  |  |  |-- cc7x_tee
|  |  |-- trng
|  |-- src
|  |  |-- proj
|  |  |  |-- cc7x_tee
|-- utils
|  |-- src
```

```
|-- cc7x_asset_prov
|   |-- examples
|   |-- lib
|-- common
|-- secure_boot_debug_utils
|   |-- cert_lib
|   |-- cert_utils
|   |-- common_utils
|   |-- x509cert_lib
|-- x509cert_utils
```

4.3 Adapt the product for your system

For information on how to adapt CryptoCell™-713 for your system, see the *Arm® CryptoCell™-713 Software Integrators Manual*.



The *Arm® CryptoCell™-713 Software Integrators Manual* is a confidential book that is only available to licensees.

4.4 Examples

The current supplied code of the integration tests is considered as reference code. You can use code snippets as examples of using the APIs of the libraries.

Once you adapt the TEE Runtime SW Integration Test Package, you can test the integration of your own platform with these tests.

5 Support

If you have any issues with the installation, content or use of this release, please create a ticket on <https://support.developer.arm.com>. Arm will respond as soon as possible.

5.1 Tools

This release has been developed with the following tools:

Table 5-1: Tools used in developing this release

Tool type	Tool name	Version
PC certificate generation tool	OpenSSL	1.0.2g 01-Mar-2016
	Python	3.5.2
Arm®v8 development board	Juno	r2
Arm®v8 compiler	GCC	7.3.0
Arm®v8 kernel	Linux Kernel Vanilla	4.19.y
Arm®v8 file system	Buildroot	2016.05rc2
Arm®v7 board	Xilinx® Zynq®-7000	706
Arm®v7 compiler	GCC	7.3.0
Arm®v7 kernel	Linux Kernel Vanilla	4.19.46
Arm®v7 file system	Buildroot	2016.05-rc2

5.2 OS

This release has been developed with the following operating system:

Table 5-2: Operating system used in developing this release

Operating system	Version
Ubuntu	16.04.2 LTS: Linux 4.13.0-32-generic x86-64