Arm® CryptoCell-703

Product revision: r0p0

OSS Release Note

Non-Confidential

PJDOC-1779577084-20327

Arm® CryptoCell-703

OSS Release Note

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 subsidiaries) 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**.

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

http://www.arm.com

Contents

1 Release overview 5
1.1 Product description 5
1.2 Release status 5
1.3 Standards compliance 5
1.4 Conventions 5
1.4.1 Glossary 6
1.4.2 Typographical conventions 7

2 Release contents 8
2.1 Deliverables 8
2.1.1 Associated products 8
2.2 Differences from previous release 8
2.3 Known limitations 8
2.3.1 Missing functionality 8
2.3.2 Open technical issues 8

3 Get started 10
3.1 Licensing information 10
3.2 Download the product 10
3.2.1 Compile the product 10
3.2.2 Directory structure 11
3.3 Adapt the product for your system 13

4 Support 14
4.1 Tools 14
4.2 OS 14

1 Release overview

1.1 Product description

The Arm® CryptoCell-703 (CryptoCell-703) Open Source Software provides a set of APIs for services provided by the product, such as:

- Cryptographic services based upon Chinese standards- SM2, SM3, and SM4.
- Content Protection Policy keys.
- TRNG definitions.
- Power management.

1.2 Release status

This is the EAC release of r0p0 Arm® CryptoCell-703 runtime software.

All planned verification and validation is complete.

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

1.3 Standards compliance

This release is compliant with the following standards:

Table 1-1 Compliant standards

Doc ID	Document title	Compliance	Version
GM/T 0009-2012	SM2 Cryptography Algorithm Application Specification	Fully	-
GB/T 0003-2012	Public Key Cryptographic Algorithm SM2 Based on Elliptic Curves - Part 1: General	Parts 1,2,3,4,5	-
GM/T 0010-2012	SM2 Cryptography Message Syntax Specification	Fully	
-	SM3 Cryptographic Hash Algorithm (December 2012)	Fully	
-	Security of the SMS4 Block Cipher Against Differential Cryptoanalysis	Fully	2005

1.4 Conventions

The following subsections describe conventions used in Arm documents.

1.4.1 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.

1.4.2 Typographical conventions

Convention	Use
italic	Introduces special terminology, denotes cross-references, and citations.
bold	Highlights interface elements, such as menu names. Denotes signal names. Also used for terms in descriptive lists, where appropriate.
`monospace`	Denotes text that you can enter at the keyboard, such as commands, file and program names, and source code.
`Monospace bold`	Denotes language keywords when used outside example code.
`monospace italic`	Denotes arguments to monospace text where the argument is to be replaced by a specific value.
`monospace underline`	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: `MRC p15, 0, <Rd>, <CRn>, <CRm>, <Opcode_2>`
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
✋	Warning
📝	Note

2 Release contents

The following sub-sections detail:

- The component parts 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.

2.1 Deliverables

Arm® CryptoCell-703 OSS includes the following deliverables:

- CryptoCell-703 TEE runtime software.
- CryptoCell-703 TEE runtime software integration tests.
- Runtime API documentation: *Arm® CryptoCell-703 Software Developers Manual*.

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

2.1.1 Associated products

The following part is available to licensees only:

- Arm® CryptoCell-703 r0p0 hardware.

The Arm® CryptoCell-703 REE Linux driver is distributed as gpl v2.0, Linux version 4.19.46.

2.2 Differences from previous release

This is the first release of CryptoCell-703 runtime software OSS.

2.3 Known limitations

Any issues known at the time of this release are detailed in the following sub-sections.

2.3.1 Missing functionality

There is no missing functionality

2.3.2 Open technical issues

The following table details any technical issues that are open at the time of this release.

Table 2-1: Defects in this release

ID	Title	Description	Workaround
-		There are no open technical issues	-

The ID is for reference only.

3 Get started

This section details any information to help you get started with accessing, setting up, and using CryptoCell-703 runtime software.

3.1 Licensing information

The Arm® CryptoCell-703 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`.

3.2 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-713-703-TEE-lib**.
- `git clone git@github.com:ARM-software/Cryptocell-713-703-TEE-Lib.git.`

3.2.1 Compile the product

- The optimization level is O2.
- All examples assume a Linux environment with Bash shell.

The following steps describe how to compile each constituent part of this product.

1. Compile the runtime library and the integration tests:
   This process assumes that the runtime software is downloaded and extracted or cloned to a working directory.
2. In the working directory, set the following environment variables:

```
% export ARCH=arm64
% export CROSS_COMPILE=<compiler_prefix>
% export COMPILER_TYPE=gcc
% export PATH=$PATH:<complier bin dir>
% export TEE_OS=linux64
% export KERNEL_DIR=<path to Linux kernel>
% export TEST_BOARD=<your-board-name>
% export TEST_AL_CONFIG_NUM=<test configuration index>
% make -C host/src/
% make -C host/src/tests/test_engine/
% make -C host/src/tests/integration_cc7x3/
```

Verify that `shared/hw/tee_include/cc_reg_base_host.h` matches the address space of the platform.

It is assumed that the environment is set correctly with a declared variable for compiling the code. For example:

```
export CROSS_COMPILE=aarch64-buildroot-linux-gnu-
export TEST_BOARD=juno
export TEST_AL_CONFIG_NUM=10
```

Table 3-1: Test board configuration numbers

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

3.2.2 Directory structure

Figure 3-1 shows the principal directory structure of this release created after unpacking the package:

Figure 3-1 Principal directory structure

```
.
|__ codesafe
|   |__ src
|       |__ crypto_api
|           |__ cc7x_sym
|           |   |__ adaptor
|           |   |__ api
|           |   |__ driver
|           |__ chinese_cert
|           |__ common
|           |__ ec_wrst
|           |   |__ ecc_domains
|           |__ pki
|           |   |__ common
|           |   |__ ec_wrst
|           |__ rnd_dma
|           |   |__ local
|           |__ sm2
|               |__ auxiliary
|               |__ dsa
|               |__ internal
|               |__ ke
|__ doxygen
|__ doxygen-it
|__ host
|   |__ src
|       |__ cc7x_teelib
|       |   |__ slim
|       |__ hal
|       |   |__ cc7x_tee
|       |__ pal
|       |   |__ cc_linux
|       |   |__ linux64
|       |   |   |__ driver
|       |   |__ no_os
|       |__ tests
|           |__ integration_cc7x3
|           |   |__ cc71x_tee
|           |__ proj
|           |   |__ cc7x
|           |__ TestAL
|           |   |__ configs
|           |   |__ hal
|           |   |   |__ include
|           |   |   |__ Juno
|           |   |   |__ Zynq
|           |   |__ pal
|           |       |__ include
|           |       |__ linux
|           |       |__ no_os
|           |__ test_engine
|           |__ tests_helper
|               |__ menu_engine
|__ shared
    |__ hw
    |   |__ tee_include
    |__ include
        |__ cc_util
        |__ crypto_api
        |   |__ cc7x_tee
        |__ pal
        |   |__ cc_linux
        |   |__ linux64
        |   |__ no_os
        |__ proj
            |__ cc7x_tee
```

3.3 Adapt the product for your system

For more information, see the *CryptoCell-703 Software Integration Manual*.

The *CryptoCell-703 Software Integration Manual* is available only to licensees of *CryptoCell-703*.

4 Support

If you have any issues with the installation, content or use of this release, please raise a ticket on **https://support.developer.arm.com**.

4.1 Supported target boards and tools

This release has been developed with the following tools:

Table 4-1: Supported target boards and tools

Description	Tools	Name	Version
Arm®v8	Board	Arm juno	r2
	Compiler	GCC	7.3.0
	Linux Kernel	Vanilla	4.19.46
	File system	Buildroot	2016.05rc2
Arm®v7	Board	xilinx zynq-7000	706
	Compiler	GCC	7.3.0
	Linux Kernel	Vanilla	4.19.46
	File system	Buildroot	2016.05-rc2

4.2 OS

This release has been developed with the following operating systems:

Table 4-2: Operating system used in developing this release

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