**Document information**

<table>
<thead>
<tr>
<th>Information</th>
<th>Content</th>
</tr>
</thead>
<tbody>
<tr>
<td>Keywords</td>
<td>i.MX RT1170, Secure JTAG.</td>
</tr>
<tr>
<td>Abstract</td>
<td>This application note describes the eFuse configuration for Secure JTAG and the authentication process, which is validated and demonstrated using the SEGGER J-Link script. Support and examples for the other Debugging tools like Lauterbach Trace32 and Arm DS5 are included in later versions.</td>
</tr>
</tbody>
</table>
1 Introduction

This document describes how the Secure JTAG on the i.MX RT1170 MCU family can be used.

The i.MX RT series JTAG Controller (JTAGC) provides a possibility to regulate the JTAG access. The three JTAG security modes are available in the i.MX RT series:

- **No debug mode**—Maximum security is provided in this mode. All security-sensitive JTAG features are permanently blocked, preventing any debug.

- **Secure JTAG mode**—High security is provided in this mode. A secret key-based challenge/response authentication mechanism is used for JTAG access.

- **JTAG Enabled mode**—Low security is provided in this mode. It is the default mode of operation for the JTAGC.

Moreover, you can also fully disable the JTAGC functionality. For configuration of these JTAG modes, One Time Programmable (OTP) eFuses are used and burned after packaging. The fuse burning process is irreversible. It is impossible to revert the fuse back to the unburned state. To explain, Secure JTAG mode is used in this document. The aim is to allow return/field testing. Authorized reactivation of the JTAG port is allowed in this mode.

There are several hardware modifications that must be made to fully enable the JTAG on RT1170-EVK. The R37, R41, R42, R43, and R44 resistors must be soldered. The R78, R187, R195, and R208 resistors must be removed. Additionally, the J5, J6, J7, and J8 jumpers must be removed. You can find the relevant resistors and jumpers in the highlighted areas in Figure 1. See the hardware design manual and the EVKB schematic for more details.
Before the Secure JTAG can be enabled, enable also the HAB and set it to the HAB Closed mode. You can find the step-by-step guide for enabling HAB in the i.MX RT1170 Secure Boot Modes Application Note (document AN13250).

CAUTION:

For previous generations of i.MX RT, it was required to burn the KTE fuse as well. The design of i.MX RT1170 is different and burning the KTE fuse locks the JTAG access forever. Do not burn the KTE fuse.

Note: This application note is based on legacy tools and flow, but the description of the secure flow within the chip still applies. We recommend using the latest tools (the MCUXpresso Secure Provisioning (SEC) Tool and SPSDK) instead of following the steps presented here. For any questions, contact your local support.
2 i.MX RT1170 Secure JTAG support

JTAG access is limited in the Secure JTAG mode by using a challenge/response-based authentication. Any access to the JTAG port is internally checked. Only the devices authorized for debugging (with the right response) can access the JTAG port. Otherwise, JTAG access is denied. The external debugger tools (such as SEGGER J-Link, Lauterbach Trace32, Arm RVDS/DS5) supporting the challenge/response-based authentication mechanism can be used. The secure JTAG mode is typically enabled in the factory manufacturing and not used during the development.

2.1 How to put the chip in Secure JTAG mode

There is only one JTAG interface on the chip with two JTAG modes. The modes can be switched via the JTAG_MOD signal (GPIO_LPSR_13 Alt0). When JTAG_MOD is in log. 0, the JTAG interface is in the debug mode and the DAP and JTAGC are enabled. When JTAG_MOD is in log. 1, the JTAG interface is in the test mode and only TESTDP is enabled. For more information, see the Chip and Arm Platform Debug Architecture chapter in the reference manual.

![System level debug architecture](image)
2.2 i.MX RT JTAGC security modes

The i.MX RT1170 JTAG Controller (JTAGC) supports three different security modes. JTAG enabled is the default mode of operation for JTAGC. The user can select the Secure JTAG mode by programming a value 0x1 to the eFuse labeled JTAG_SMODE, described in Table 1. The eFuse has the default value 0x0, which means that the JTAG controller is unsecured by default. Further details on eFuses are available in the Fusemap and On-Chip OTP Controller (OCOTP_CTRL) chapters in the appropriate SRM_RT1170 Security Reference Manual for the i.MX RT1170 available at [www.nxp.com](http://www.nxp.com) upon a request.

To lock a specific fuse word and prevent further modifications to all the fuses inside the fuse word, set the WORDLOCK bit of the OCOTP register to 0x1 before writing into one of the fuses inside the chosen word. When the writing operation is completed, the whole word is prevented from changing forever.

For more information, see the Bank redundancy vs ECC and Lock Bits chapters of the i.MX RT1170 Processor Reference Manual (document IMXRT1170RM).

Note: Programming these fuses disables access to functions and JTAG Security Mode fuse bits. Users must ensure that it is programmed last, once the final fuse configuration has been decided.

Table 1. eFuses associated with the Secure JTAG feature

<table>
<thead>
<tr>
<th>Addr[bits]</th>
<th>Fuse Name</th>
<th>Fuse Function</th>
<th>Settings</th>
</tr>
</thead>
<tbody>
<tr>
<td>0x960[9]</td>
<td>JTAG_HEO</td>
<td>JTAG HAB Enable Override. Disallows HAB JTAG enabling. The HAB may normally enable JTAG debugging with the HAB_JDE-bit in the OCOTP SCS register. The JTAG_HEO-bit can override this behavior.</td>
<td>0 - HAB may enable JTAG debug access 1 - HAB JTAG enable is overridden (HAB may not enable JTAG debug access)</td>
</tr>
<tr>
<td>0x960[1]</td>
<td>SEC_CONFIG[1]</td>
<td>Security Configuration Mode (together with SEC_CONFIG[0])</td>
<td>SEC_CONFIG[1:0]: 00 - FAB (Open) 01 - Open - allows any code to be flashed and executed, even if it has no valid signature. 1x - Closed (Security On) This is programmed during the HAB enablement phase (By setting the HAB Closed mode)</td>
</tr>
<tr>
<td>0x960[7:6]</td>
<td>JTAG_SMODE[1:0]</td>
<td>JTAG Security Mode. Controls the security mode of the JTAG debug interface</td>
<td>00 - JTAG enable mode (Default) 01 - Secure JTAG mode 11 - No debug mode</td>
</tr>
<tr>
<td>0x960[11]</td>
<td>JTAG_DISABLE</td>
<td>Additional JTAG mode with the highest level of JTAG protection, overriding the JTAG_SMODE eFuses. In this mode, all JTAG features are disabled, including Secure JTAG and Boundary Scan</td>
<td>0 - JTAG is enabled 1 - JTAG is disabled</td>
</tr>
</tbody>
</table>
Table 1. eFuses associated with the Secure JTAG feature...continued

<table>
<thead>
<tr>
<th>Addr[bits]</th>
<th>Fuse Name</th>
<th>Fuse Function</th>
<th>Settings</th>
</tr>
</thead>
</table>
| 0x880[14:11]| JTAG_RESP_RLOCK[3:0] | JTAG_RESP_RLOCK[0]: Read lock of JTAG_RESP[31:0]                           | Read Lock  
  0000 - Unlock (The controlled field can be read in the corresponding IIM register.)  
  1111 - Lock (The controlled field cannot be read in the corresponding IIM register.)  
  others - must not be set |
|             |                   | JTAG_RESP_RLOCK[1]: Read lock of JTAG_RESP[63:32]                           |                                                                          |
|             |                   | JTAG_RESP_RLOCK[2]: Read lock of JTAG_RESP[95:64]                            |                                                                          |
|             |                   | JTAG_RESP_RLOCK[3]: Read lock of JTAG_RESP[127:96]                           |                                                                          |
| 0xCB0-0xCE0 | JTAG_RESP[127:0]  | Response reference value for the secure JTAG controller                     | -                                                                       |

Note:

The level of security cannot be reduced but only increased. Since debug modes are controlled by OTP (Hardware fuses), bits can only be blown once.

For example, the following mode changes are possible:

- “JTAG Enabled” to “Secure JTAG”
- “Secure JTAG” to “No debug”

2.3 Secure JTAG eFuses

The challenge/response mechanism used to authenticate the JTAG access uses a challenge value and the associated secret response key. The keys are stored in eFuses inside the IC. The i.MX RT1170 series eFuses used to store the challenge value and the secret response key are listed below:

- The challenge value is the “Device Unique ID” that is programmed into the eFuses. This Device ID is unique for each IC and can be read from the OCOTP registers by their Fuse Row Index as follows: OCOTP->FUSE016 and OCOTP->FUSE017. The eFuses are programmed during manufacturing.
- The user program the secret response key (128 bits) into the eFuses marked JTAG_RESP.

After programming the secret response key, the user must disable the ability of software running on the Arm core to read or overwrite the response key. It is done by programming 0x1111 to the associated lock eFuse JTAG_RESP_RLOCK.

The definition of the response value is left to the user. The Arm core cannot read the value once the response fuse field is provisioned and locked.

2.4 SW enabled JTAG

The Secure JTAG authentication may be bypassed in SW by writing logic 1 to HAB_JDE (HAB JTAG DEBUG ENABLE) bit in the e-fuse controller module. The JTAG is opened, regardless of its security mode. The S/W JTAG enable allows JTAG enabling without activating the Challenge-Response mechanism.

The platform initialization software should set the LOCK bit for the JDE bit before transferring control to the application code to ensure that only the trusted SW can set the JDE bit.

The JTAG SW enable does not allow debug in case of boot or memory fault as it requires a reset before entering debug.
The JTAG_JDE bit SW enable backdoor access can be permanently disabled by burning the JTAG_HEO fuse.

**Note:** The S/W enabled JTAG feature reduces the overall security level of the system as it relies on S/W protections. If this feature is not required, it is recommended to burn the JTAG_HEO e-fuse that disables this feature.

### 2.4.1 JDE bit control in HAB (High Assurance Boot)

The HAB_JDE can be set to logic 1 by ROM boot SW after unlocking by the Authenticate CSF command.

Before generating of the signed program image, the user must edit the UNLOCK section in the .sb file and provide the device-specific UID in the proper format as a sequence of 8 bytes, see the below example for UID = 0x63e1841b440b81d2:

```c
section (SEC_UNLOCK;
Unlock_Engine = "OCOTP",
Unlock_features = "JTAG, SCS, SRK REVOKE",
Unlock_UID = "0xe1, 0x63, 0x1b, 0x84, 0x0b, 0x44, 0xd2, 0x81"
)
```

For more information about the HAB_JDE SW control by platform initialization SW in HAB (High Assurance Boot) refer to section 5.2.13 Unlock (HAB only) in [5].

### 2.5 Secure JTAG debug authentication protocol

When the JTAGC is in the secure debug mode, the authentication process is as follows:

1. JTAG shifts the challenge key through the Test Data Output (TDO) chain.
2. On the host side, the debug tool takes the challenge key as an input and generates the expected response key.
3. The associated response key is shifted back through the Test Data Input (TDI) chain.
4. The JTAGC compares the expected internal fused response key with the one shifted in and enables the JTAG access only if it matches.

**Note:**

Any device reset after JTAG access authorization shifts the JTAG controller back to its locked state.

*Figure 3* shows how the challenge/response mechanism works with the JTAG tools.
The JTAG debug tool passes the retrieved challenge key to the user application and gets the associated response key in return. The management of the challenge/response pairs is user-dependent and not handled by NXP or the debug tool vendors. Key management is discussed further in Section 3.

2.6 JTAGC disable fuse

In addition to the various JTAG security modes implemented internally in the JTAGC, there is an option to disable the JTAGC functionality with the JTAG_DISABLE eFuse. This eFuse creates an additional JTAG mode, JTAG Disabled with the highest level of JTAG protection, overriding the JTAG_SMODE eFuses. In this mode all JTAG features are disabled, including Secure JTAG and Boundary Scan; users must ensure that this fuse is not blown if they wish to use the Secure JTAG functionality.

3 Secret response key approaches

For every challenge value (“Device Unique ID” in i.MX RT1170) that is retrieved with a JTAG instruction, there is an associated secret response key known only by the user. The JTAG tool vendor only handles the JTAG mechanism used by this authentication process, and does not know the secret response key value programmed into the eFuses. It is left to the user to determine the level of protection that is put in place.
The following are policies for secret response key management by the user application.

1. **Identical Response Keys** — The same response key is used for each chip. The user can choose a response key that is fused in all chips. It is the simplest, but least sophisticated usage from a security point of view. If an unauthorized user gains access to the fused response key, all the products fused with this response key can be accessed through the JTAG port.

2. **Database of Unique Response Keys** — The user maintains a database of all generated response keys. The user application can look up the table based on the challenge value. It is possible to implement a secure server holding the challenge/response pairs authenticating the user but it requires an independent implementation effort. The challenge values for all ICs must be read and a database of matching challenge response pairs must be built. Storing and managing numerous response keys is not trivial, but advantageous from a security standpoint, as it does not rely on any breakable algorithms.

3. **Algorithmically Generated Response Keys** — Response keys are generated based on an algorithm. With this method, there is no large database to manage. For instance, the challenge value can be used by the algorithm to generate a response key. This response key is programmed into JTAG_RESP eFuses. Then, every time the challenge value is retrieved through JTAG, it can be processed by the user application and used to generate the expected response key for the JTAG debug tools. Once the algorithm is exposed or reverse-engineered, this method is no longer secure.

**Note:** NXP does not provide secure response key management or key generation services; these topics are not within the scope of this document.

### 3.1 Programming Secure JTAG eFuses using the NXP tool

To program the relevant eFuses needed for Secure JTAG on the chip, the user must first follow the steps below. Information on the On-Chip OTP Controller (OCOTP_CTRL) and the Fusemap can be found in the appropriate i.MX RT1170 series reference manual available at [http://www.nxp.com](http://www.nxp.com).

2. Enable the HAB and set the security configuration mode to HAB closed (see the step-by-step guide in the i.MX RT1170 security application note).
3. The user must program the values below to the eFuses needed for secure JTAG:
   - Read and back-up the 64-bit "Challenge" value stored in the eFuse UUID[1,0], location (0x900, 0x910).
   - Program a 128-bit (16 Bytes) secret response key in the eFuse JTAG_RESP, location (0xcb0-0xce0). In the example below, value `0x12345678123456781234567812345678` is programmed.
   - Program b'01 in the eFuse JTAG_SMODE (0x960[7:6]) to switch the JTAGC to Secure JTAG mode.
   - Finally, the user must program 0x1 in the eFuse to disable read/write access of the secret response key. After this operation, the secret response field “JTAG_RESP” becomes "invisible" in the fuse map.

To have the Secure JTAG enabled, follow the steps mentioned above in **Section 3.1** and see **Table 1** for more details about the appropriate eFuse bits.

**CAUTION:**

*For previous generations of i.MX RT, it was required to burn the KTE fuse as well. The design of i.MX RT1170 is different and burning the KTE fuse locks the JTAG access forever. Do not burn the KTE fuse.*

### 4 Debugging with the Secure JTAG enabled

To use the Secure JTAG feature, the JTAG debugger must support it. The example provided in this section uses the SEGGER J-Link debug tool.

The following steps assume that users have experience working with the debug tools.
4.1 Steps to connect J-Link debugger via Secure JTAG

The following steps connect the SEGGER J-Link debug tool to the i.MX RT1170 when using Secure JTAG:

1. Download the SEGGER J-Link Software and documentation pack:
   
   
   If you wish to navigate to these scripts from SEGGER main page for reference, they are located under Downloads -> J-Link / J-Trace -> J-Link Software and Documentation Pack.

2. Download and edit the file J-Link script file named “NXP_RT1170_SecureJTAG.JlinkScript”. The script file is at the end of this application note or at the documentation page for the RT1170 device (file AN13133SW). In this file, add the secret response key that was programmed into the JTAG_RESP eFuse. In the following example, the secret response key is “0x12345678123456781234567812345678”, and matches the response key programmed in the eFuses in Section 3.1.

   // Secure response stored @ 0xcb0-0xce0 in eFUSE region (OTP memory)
   Key0 = 0x12345678;
   Key1 = 0x12345678;
   Key2 = 0x12345678;
   Key3 = 0x12345678;

3. Locate the SEGGER SW J-Link installation directory.

4. Run the “jlink.exe” with the mentioned script file as a parameter.

   For instance:
   
   jlink.exe -JLinkScriptFile NXP_RT1170_SecureJTAG.JlinkScript -device CORTEX-M7 -if JTAG -speed 4000 -autoconnect 1 -JTAGConf -1,-1
   
   **Note:** The external IDE tool can call “JLinkGDBServer.exe” application with the same script file to unsecure the target.

   The tool script should read the Challenge value from eFUSE UUID[1,0] location. And it provides the appropriate Response from for JTAGC for authentication match.

   The debug tool should successfully attach to the i.MX RT1170 target over JTAG. The screen capture in Figure 4 shows a successful attach over Secure JTAG:
Connecting to target via JTAG
InitTarget() start
TotalIRlen = 4, IRPrint = 0x01
JTAG chain detection found 1 devices:
  #0 Id: 0x888C001D, IRLen: 04, JTAG-DP
Challenge UUID: 0x82967D6A
Challenge UUID: 0x3218080E
InitTarget() end
TotalIRlen = 4, IRPrint = 0x01
JTAG chain detection found 1 devices:
  #0 Id: 0x888C001D, IRLen: 04, JTAG-DP
DPv0 detected
Scanning AP map to find all available APs
AP[3]: Stopped AP scan as end of AP map has been reached
AP[0]: AHB-AP (IDR: 0x84770001)
AP[1]: AHB-AP (IDR: 0x24770011)
AP[2]: APB-AP (IDR: 0x54770002)
Iterating through AP map to find AHB-AP to use
AP[0]: Core found
AP[0]: AHB-AP ROM base: 0x0060D000
CPUID register: 0x411FC272. Implementer code: 0x41 (ARM)
Found Cortex-M7 MP12, Little endian.
FPUnit: 8 code (BP) slots and 0 literal slots
Coresight components:
ROMTbl[0] @ E0000000
ROMTbl[0][0]: E0000000, CID: B105100D, PID: 000BB4C8 ROM Table
ROMTbl[1] @ E00FF000
ROMTbl[1][0]: E00FF000, CID: B105100D, PID: 000BB4C7 ROM Table
ROMTbl[2] @ E00FF000
ROMTbl[2][0]: E00FE000, CID: B105E00D, PID: 000BB00C SCS-M7
ROMTbl[2][1]: E0001000, CID: B105E00D, PID: 000BB002 DWT
ROMTbl[2][2]: E0002000, CID: B105E00D, PID: 000BB00E FPB-M7
ROMTbl[2][3]: E0000000, CID: B105E00D, PID: 000BB001 ITM
ROMTbl[1][1]: E0041000, CID: B105900D, PID: 001BB975 ETM-M7
ROMTbl[1][2]: E0042000, CID: B105900D, PID: 004BB906 CTI
ROMTbl[0][1]: E0043000, CID: B105900D, PID: 001BB908 CSTF
Cache: Separate I- and D-cache.
I-Cache L1: 32 KB, 512 Sets, 32 Bytes/Line, 2-Way
D-Cache L1: 32 KB, 256 Sets, 32 Bytes/Line, 4-Way
Cortex-M7 identified.
J-Link>

Figure 4. SEGGER J-Link successfully connected to Secured JTA
Users can now perform normal JTAG debugger operations, as the device has been authenticated using the Challenge-Response mechanism.

**Note:**

Any reset after JTAG access authorization shifts the JTAG controller back to its lock state, requiring that this authentication process is repeated.

5. To ensure that i.MX RT series JTAGC is operating in secure mode, edit the “NXP_RT1170_SecureJTAG.JlinkScript” file, provide an incorrect response key, and rerun the script. The debug tool should fail to attach to the i.MX RT1170 target over JTAG.

### 4.2 Example of SEGGER J-link Secure JTAG unlock script

```c
int InitTarget(void) {
    int v;
    int Key0;
    int Key1;
    int Key2;
    int Key3;
    // Secure response stored @ [0xcb0-0xce0] in eFUSE region (OTP memory)
    Key0 = 0x12345678;
    Key1 = 0x12345678;
    Key2 = 0x12345678;
    Key3 = 0x12345678;
    JLINK_CORESIGHT_Configure("IRPre=0;DRPre=0;IRPost=0;DRPost=0;IRLenDevice=4");
    CPU = CORTEX_M7;
    JLINK_SYS_Sleep(100);
    JLINK_JTAG_WriteIR(0x9); // Output Challenge instruction
    // Readback Challenge, Shift 64 dummy bits on TDI
    JLINK_JTAG_StartDR();
    JLINK_SYS_Report("Reading Challenge ID....");
    // 32-bit dummy write on TDI / read 32 bits on TDO
    JLINK_JTAG_WriteDRCont(0xffffffff, 32);
    v = JLINK_JTAG_GetU32(0);
    JLINK_SYS_Report1("Challenge UUID0:", v);
    JLINK_JTAG_WriteDREnd(0xffffffff, 32);
    v = JLINK_JTAG_GetU32(0);
    JLINK_SYS_Report1("Challenge UUID1:", v);
    JLINK_JTAG_WriteIR(0x1); // Output Response instruction
    JLINK_JTAG_StartDR();
    JLINK_JTAG_WriteDRCont(Key0, 32);
    JLINK_JTAG_WriteDRCont(Key1, 32);
    JLINK_JTAG_WriteDRCont(Key2, 32);
    JLINK_JTAG_WriteDREnd(Key3, 32);
    return 0;
}
```

### 5 Conclusion

This application note describes the eFuse configuration for Secure JTAG and the authentication process, which is validated and demonstrated using the SEGGER J-Link script. Support and examples for the other Debugging tools like Lauterbach Trace32 and Arm DSS are included in later versions.
6 References

1. Configuring Secure JTAG for the i.MX 6 Series Family of Application Processors (document AN4686)
4. Training JTAG Interface, Lauterbach TRACE32 (document Training JTAG Interface)
5. HAB Code-Signing Tool User’s Guide (Rev. 3.2.0, 04/2019) (document IMX_CST3.2.0_TOOL)

7 Note about the source code in the document

Example code shown in this document has the following copyright and BSD-3-Clause license:

Copyright 2023 NXP Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials must be provided with the distribution.
3. Neither the name of the copyright holder nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

8 Revision history

Table 2 summarizes the revisions to this document.

<table>
<thead>
<tr>
<th>Revision number</th>
<th>Release date</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>5</td>
<td>7 November 2023</td>
<td>The document is updated to correspond to the latest guidelines, Section 1 is updated.</td>
</tr>
<tr>
<td>4</td>
<td>21 September 2023</td>
<td>The document is updated to correspond to the latest guidelines, Section 1 is updated.</td>
</tr>
<tr>
<td>3</td>
<td>23 February 2022</td>
<td>Updated Section 1.</td>
</tr>
<tr>
<td>2</td>
<td>08 December 2021</td>
<td>Updated Section 1 and Section 3.1.</td>
</tr>
<tr>
<td>1</td>
<td>28 July 2021</td>
<td>Updated links to external resources and clarified some information.</td>
</tr>
<tr>
<td>0</td>
<td>February 2021</td>
<td>Initial public release</td>
</tr>
</tbody>
</table>

1 The document is available upon request at www.nxp.com.
Definitions

Draft — A draft status on a document indicates that 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 in a draft version of a document and shall have no liability for the consequences of use of such information.

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.

Terms and conditions of commercial sale — NXP Semiconductors products are sold subject to the general terms and conditions of commercial sale, as published at https://www.nxp.com/profile/terms, unless otherwise agreed in a valid written individual agreement. In case an individual agreement is concluded only the terms and conditions of the respective agreement shall apply. NXP Semiconductors hereby expressly objects to applying the customer’s general terms and conditions with regard to the purchase of NXP Semiconductors products by customer.

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.

Suitability for use in non-automotive qualified products — Unless this document expressly states that this specific NXP Semiconductors product is automotive qualified, the product is not suitable for automotive use. It is neither qualified nor tested in accordance with automotive testing or application requirements. NXP Semiconductors accepts no liability for inclusion and/or use of non-automotive qualified products in automotive equipment or applications.

In the event that customer uses the product for design-in and use in automotive applications to automotive specifications and standards, customer (a) shall use the product without NXP Semiconductors’ warranty of the product for such automotive applications, use and specifications, and (b) whenever customer uses the product for automotive applications beyond NXP Semiconductors’ specifications such use shall be solely at customer’s own risk, and (c) customer fully indemnifies NXP Semiconductors for any liability, damages or failed product claims resulting from customer design and use of the product for automotive applications beyond NXP Semiconductors’ standard warranty and NXP Semiconductors’ product specifications.

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

Security — Customer understands that all NXP products may be subject to unidentified vulnerabilities or may support established security standards or specifications with known limitations. Customer is responsible for the design and operation of its applications and products throughout their lifecycles to reduce the effect of these vulnerabilities on customer’s applications and products. Customer’s responsibility also extends to other open and/or proprietary technologies supported by NXP products for use in customer’s applications. NXP accepts no liability for any vulnerability. Customer should regularly check security updates from NXP and follow up appropriately.

Customer shall select products with security features that best meet rules, regulations, and standards of the intended application and make the ultimate design decisions regarding its products and is solely responsible for compliance with all legal, regulatory, and security related requirements concerning its products, regardless of any information or support that may be provided by NXP.

NXP has a Product Security Incident Response Team (PSIRT) (reachable at PSIRT@nxp.com) that manages the investigation, reporting, and solution release to security vulnerabilities of NXP products.

NXP B.V. — NXP B.V. is not an operating company and it does not distribute or sell products.

Trademarks

Notice: All referenced brands, product names, service names, and trademarks are the property of their respective owners. NXP — wordmark and logo are trademarks of NXP B.V.

Legal information

Draft — A draft status on a document indicates that 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 in a draft version of a document and shall have no liability for the consequences of use of such information.
1 Introduction ......................................................2
2 i.MX RT1170 Secure JTAG support ................ 4
  2.1 How to put the chip in Secure JTAG mode ...... 4
  2.2 i.MX RT JTAGC security modes ................... 5
  2.3 Secure JTAG eFuses ................................... 6
  2.4 SW enabled JTAG .................................... 6
  2.4.1 JDE bit control in HAB (High Assurance Boot) ........................................... 7
  2.5 Secure JTAG debug authentication protocol ...... 7
  2.6 JTAGC disable fuse .................................... 8
3 Secret response key approaches ..................... 8
  3.1 Programming Secure JTAG eFuses using
      the NXP tool ............................................ 9
4 Debugging with the Secure JTAG enabled .......... 9
  4.1 Steps to connect J-Link debugger via Secure JTAG ........................................... 10
  4.2 Example of SEGGER J-link Secure JTAG unlock script ........................................ 12
5 Conclusion .................................................... 12
6 References ................................................... 13
7 Note about the source code in the document ........................................... 13
8 Revision history ............................................ 13
  Legal information ........................................... 14