AG35 Series QuecOpen Secure Boot Memory Dump Capture Guide

Automotive Module Series

Version: 1.0

Date: 2020-08-19

Status: Released

www.quectel.com

Our aim is to provide customers with timely and comprehensive service. For any assistance, please contact our company headquarters:

Quectel Wireless Solutions Co., Ltd.
Building 5, Shanghai Business Park Phase III (Area B), No.1016 Tianlin Road, Minhang District, Shanghai 200233, China
Tel: +86 21 5108 6236 Email: info@quectel.com

Or our local office. For more information, please visit: http://www.quectel.com/support/sales.htm.

For technical support, or to report documentation errors, please visit:
http://www.quectel.com/support/technical.htm or email to support@quectel.com.

GENERAL NOTES

QUECTEL OFFERS THE INFORMATION AS A SERVICE TO ITS CUSTOMERS. THE INFORMATION PROVIDED IS BASED UPON CUSTOMERS' REQUIREMENTS. QUECTEL MAKES EVERY EFFORT TO ENSURE THE QUALITY OF THE INFORMATION IT MAKES AVAILABLE. QUECTEL DOES NOT MAKE ANY WARRANTY AS TO THE INFORMATION CONTAINED HEREIN, AND DOES NOT ACCEPT ANY LIABILITY FOR ANY INJURY, LOSS OR DAMAGE OF ANY KIND INCURRED BY USE OF OR RELIANCE UPON THE INFORMATION. ALL INFORMATION SUPPLIED HEREIN IS SUBJECT TO CHANGE WITHOUT PRIOR NOTICE.

DISCLAIMER

WHILE QUECTEL HAS MADE EFFORTS TO ENSURE THAT THE FUNCTIONS AND FEATURES UNDER DEVELOPMENT ARE FREE FROM ERRORS, IT IS POSSIBLE THAT THESE FUNCTIONS AND FEATURES COULD CONTAIN ERRORS, INACCURACIES AND OMISSIONS. UNLESS OTHERWISE PROVIDED BY VALID AGREEMENT, QUECTEL MAKES NO WARRANTIES OF ANY KIND, IMPLIED OR EXPRESS, WITH RESPECT TO THE USE OF FEATURES AND FUNCTIONS UNDER DEVELOPMENT. TO THE MAXIMUM EXTENT PERMITTED BY LAW, QUECTEL EXCLUDES ALL LIABILITY FOR ANY LOSS OR DAMAGE SUFFERED IN CONNECTION WITH THE USE OF THE FUNCTIONS AND FEATURES UNDER DEVELOPMENT, REGARDLESS OF WHETHER SUCH LOSS OR DAMAGE MAY HAVE BEEN FORESEEABLE.

COPYRIGHT

About the Document

Revision History

Version	Date	Author	Description
1.0	2020-08-19	Darren LI	Initial

Contents

1 Introduction

In Quectel AG35 series module, a memory dump file is primarily used for identifying a problem or an error within the Linux OS. Typically, such a file provides information about the state of the system at the time of a crash or an abnormal termination. The information consists of memory locations, program state and other related details.

In QuecOpen® solution, AG35 series supports Secure Boot. The memory dump is blocked by default for security when Secure Boot is enabled. To better satisfy your requirements, AG35 series allows you to capture the memory dump even in QuecOpen® solution.

This document introduces how to capture the memory dump of Quectel AG35 series module in QuecOpen® solution when Secure Boot is enabled, with major steps and the test method detailed.

2 Steps to Capture Memory Dump

If the memory dump is required in QuecOpen® solution, the module allows you to capture it by modifying the configuration file in the sighing tool, re-signing the firmware and downloading the re-signed firmware to overwrite the previous one. See the following sections for the illustration of every step.

2.1. Modify Configuration File in the Signing Tool

2.1.1. Read SN of the Chip

Find the chip's SN under the path *cat/sys/devices/soc0/serial_number* in the file system of the module and transfer it into hexadecimal format.

2.1.2. Modify Configuration File in the Signing Tool

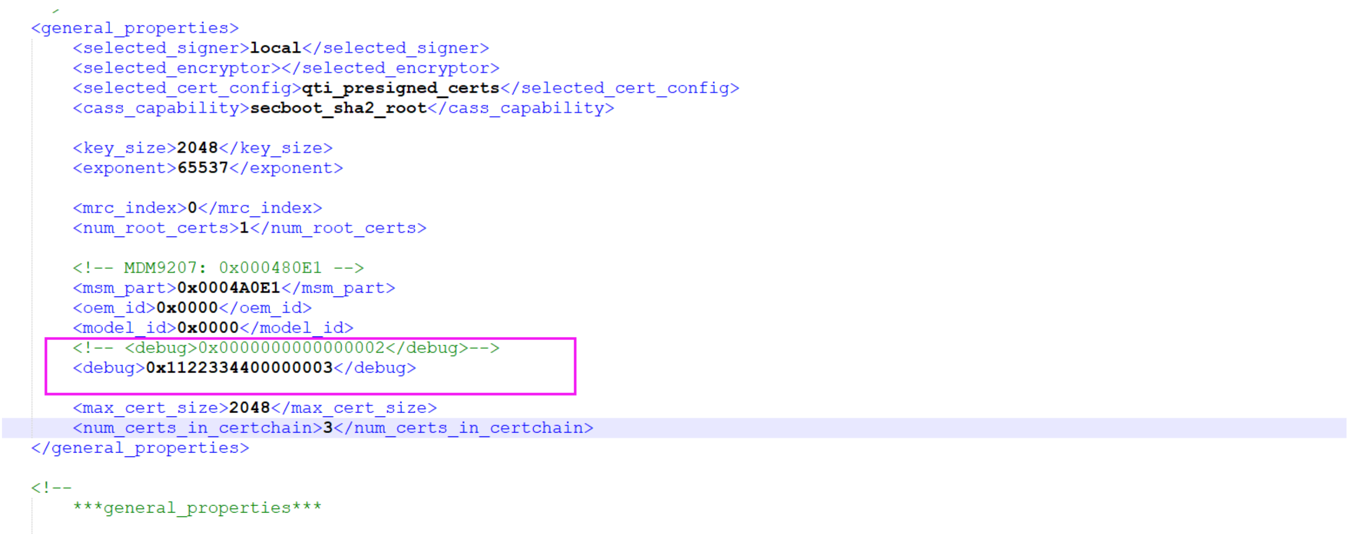
Modify the configuration file in the signing tool, namely to write into it the hexadecimal SN.

The configuration file is located in *common\sectools\config\9x07\9x07_secimage.xml* in the signing tool package.

Take the hexadecimal SN 0x11223344 as an example, the modification of the file is illustrated as below:

1. Modify the <debug> parameter.

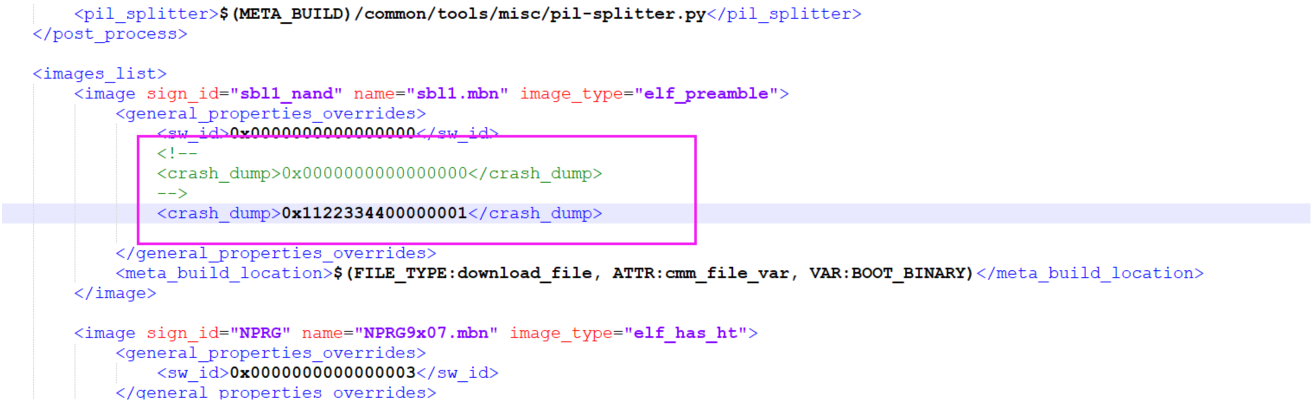
Replace the high byte in **<debug>** with the hexadecimal SN and the low byte with the number 3. In this case, the modified parameter should be 0x1122334400000003.



```
<general_properties>
    <selected_signer>local</selected_signer>
    <selected_encryptor></selected_encryptor>
    <selected_cert_config>qti_presigned_certs</selected_cert_config>
    <cass_capability>secboot_sha2_root</cass_capability>

    <key_size>2048</key_size>
    <exponent>65537</exponent>

    <mrc_index>0</mrc_index>
    <num_root_certs>1</num_root_certs>

    <!-- MDM9207: 0x000480E1 -->
    <msm_part>0x0004A0E1</msm_part>
    <oem_id>0x0000</oem_id>
    <model_id>0x0000</model_id>
    <!-- <debug>0x0000000000000002</debug>-->
    <debug>0x1122334400000003</debug>

    <max_cert_size>2048</max_cert_size>
    <num_certs_in_certchain>3</num_certs_in_certchain>
</general_properties>

<!--
    ***general_properties***
```

2. Modify the <crash dump> parameter.

Replace the high byte in **<crash dump>** with the hexadecimal SN and the low byte with the number 1. In this case, the modified parameter should be 0x1122334400000001.



```
    <pil_splitter>$(META_BUILD)/common/tools/misc/pil-splitter.py</pil_splitter>
</post_process>

<images_list>
    <image sign_id="sbl1_nand" name="sbl1.mbn" image_type="elf_preamble">
        <general_properties_overrides>
            <sw_id>0x0000000000000000</sw_id>
            <!--
            <crash_dump>0x0000000000000000</crash_dump>
            -->
            <crash_dump>0x1122334400000001</crash_dump>

        </general_properties_overrides>
        <meta_build_location>$(FILE_TYPE:download_file, ATTR:cmm_file_var, VAR:BOOT_BINARY)</meta_build_location>
    </image>

    <image sign_id="NPRG" name="NPRG9x07.mbn" image_type="elf_has_ht">
        <general_properties_overrides>
            <sw_id>0x0000000000000003</sw_id>
        </general_properties_overrides>
```

2.2. Re-sign Firmware

Re-sign the firmware after modifying the configuration file.

This step entails the using of a signing tool released by Quectel. For further guidance on this step, see the user guide provided along with the signing tool which you can get from Quectel Technical Support (support@quectel.com).

2.3. Download Firmware

Download the newly signed firmware to the module to overwrite the previously signed one. Contact Quectel Technical Support (support@quectel.com) for the firmware downloading tool.

2.4. Test and Capture

After downloading the re-signed firmware, you can test whether the configurations are correct – whether the memory dump capture mode is enterable – by executing the following commands in Linux system:

```
echo 0 > /sys/bus/msm_subsys/devices/subsys1/system_reset_mode
echo   system >   /sys/bus/msm_subsys/devices/subsys1/restart_level
echo c > /proc/sysrq-trigger
```

Of these three commands, the first and second ones configure the system to enter into memory dump mode in the case of an exception; the third one is used to trigger a panic.

If the configurations mentioned in previous steps are correct and the re-signed firmware is downloaded successfully, the module will reserve only one DM USB virtual serial port through which the memory dump information can be captured after connecting the module with QPST. Contact Quectel Technical Support (support@quectel.com) for QPST.

3 Appendix A References

Table 1: Terms and Abbreviations

Abbreviation	Description
DM	Device Manager
QPST	Qualcomm Product Support Tool
SN	Serial Number
USB	Universal Serial Bus