

# **BG95&BG77&BG600L**

## **Series Secure Boot**

### **Application Note**

**LPWA Module Series**

Version: 1.0

Date: 2020-12-02

Status: Released

**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](mailto: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](mailto: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.

## **Duty of Confidentiality**

The Receiving Party shall keep confidential all documentation and information provided by Quectel, except when the specific permission has been granted by Quectel. The Receiving Party shall not access or use Quectel's documentation and information for any purpose except as expressly provided herein. Furthermore, the Receiving Party shall not disclose any of the Quectel's documentation and information to any third party without the prior written consent by Quectel. For any noncompliance to the above requirements, unauthorized use, or other illegal or malicious use of the documentation and information, Quectel will reserve the right to take legal action.

## Copyright

The information contained here is proprietary technical information of Quectel Wireless Solutions Co., Ltd. Transmitting, reproducing, disseminating and editing this document as well as using the content without permission are forbidden. Offenders will be held liable for payment of damages. All rights are reserved in the event of a patent grant or registration of a utility model or design.

*Copyright © Quectel Wireless Solutions Co., Ltd. 2020. All rights reserved.*

# About the Document

## Revision History

Version	Date	Author	Description
-	2020-11-03	Harding HU	Creation of the document
1.0	2020-12-02	Harding HU	First official release

---

## Contents

About the Document .....	3
Contents .....	4
Table Index .....	5
Figure Index .....	6
<b>1 Introduction .....</b>	<b>7</b>
1.1. Applicable Modules .....	7
<b>2 Secure Boot Overview .....</b>	<b>8</b>
2.1. Definition .....	8
2.2. Secure Boot Process .....	8
2.3. Certificate Chain .....	9
2.4. Image Signing .....	9
2.5. Hardware Foundation .....	9
2.6. Secure Boot Toolkit .....	10
2.7. sec.elf .....	11
<b>3 Enable Secure Boot .....</b>	<b>12</b>
3.1. Procedure .....	12
3.2. Verification .....	13
3.2.1. AT+QSECBOOTSTAT? Query Secure Boot Status .....	13
<b>4 Appendix A References .....</b>	<b>14</b>

## Table Index

Table 1: Applicable Modules.....	7
Table 2: Related Documents .....	14

## Figure Index

Figure 1: Quectel SecBootTools ..... 10

# 1 Introduction

This document describes details of Secure Boot and how to enable this function of Quectel BG95 series, BG77 and BG600L-M3 modules.

## 1.1. Applicable Modules

Table 1: Applicable Modules

Module Series	Model	Description
<b>BG95 Series</b>	BG95-M1	Cat M1
	BG95-M2	Cat M1/Cat NB2
	BG95-M3	Cat M1/Cat NB2/EGPRS
	BG95-M4	Cat M1/Cat NB2, 450 MHz Supported
	BG95-M5	Cat M1/Cat NB2/EGPRS, Power Class 3
	BG95-M6	Cat M1/Cat NB2, Power Class 3
	BG95-MF	Cat M1/Cat NB2, Wi-Fi Positioning
<b>BG77</b>	BG77	Cat M1/Cat NB2
<b>BG600L</b>	BG600L-M3	Cat M1/Cat NB2/EGPRS

### NOTE

Hereinafter, BG95 series is collectively called BG95 unless otherwise specified.



# 2 Secure Boot Overview

## 2.1. Definition

Secure Boot is defined as a boot sequence in which each firmware image that is loaded and executed is authorized using the firmware that was previously authorized.

At each stage of Secure Boot process, signature verification is performed to prevent any software without valid signature or maliciously modified software from running on the module. A root trusted entity is needed during the boot process. The Primary Boot Loader (PBL), embedded in the module as a firmware, is unmodifiable, and therefore can serve as the root trusted entity.

## 2.2. Secure Boot Process

The Secure Boot process comprises multiple stages, and each image in every stage performs a specific function. After the Secure Boot is enabled, the image to be executed in each stage needs to be verified by the image that was previously verified. If the verification fails, the entire boot process stops and the module cannot boot up. Quectel BG95, BG77 and BG600L-M3 modules follow the verification sequence of Primary Boot Loader (PBL) → Secondary Boot Loader (SBL) → ARM® TrustZone.

- As the root of trust, the PBL (also known as RoT) is the firmware embedded in chips and cannot be modified. Therefore, it is considered as the most trusted entity in the boot process, and performs authentication on the image to be executed in the next boot stage.
- The SBL is usually verified in the second boot stage. After it is successfully authenticated by the PBL, it can be executed and used to authenticate the image in the next stage.

### NOTE

Secure Boot is disabled by default. For details on how to enable Secure Boot, see **Chapter 3**.

## 2.3. Certificate Chain

Secure Boot supports 2048-bit or 4096-bit RSA private keys for signatures of the certificate and images. The format of the certificate signatures meets the *PKCS #1 v1.5* or *ITU-T X.509 v3* Standard and the SHA1 or SHA256 algorithm.

The certificate chain of Quectel BG95, BG77 and BG600L-M3 modules consists of two certificates in X.509 format and based on SHA-384 algorithm: the self-signed root certificate and the attestation certificate.

The required certificates can be generated through the *gencerts.bat* mentioned in **Chapter 2.6**. The generated certificates are used to sign the image and the *sec.elf* file (see **Chapter 2.7** for details).

## 2.4. Image Signing

During Secure Boot, the images to be executed in each boot stage have to be signed first. Quectel firmware images use the standard ELF format, and each image includes several segments indicating different types of information separately, wherein the *hash table segment* stores signature related information. The *hash table segment* also includes the hash values of each segment and the information about certificate trust chain.

The images listed below have to be signed in Secure Boot process for Quectel BG95, BG77 and BG600L-M3 modules.

- *sb11.mbn*
- *prog\_firehose\_nand\_mdm9x05.elf*
- *tz.mbn*
- *devcfg.mbn*
- *rpm.mbn*
- *multi\_image.mbn*
- *qdsp6sw.mbn*
- *qdsp6sw\_2.mbn*
- *apps.mbn*

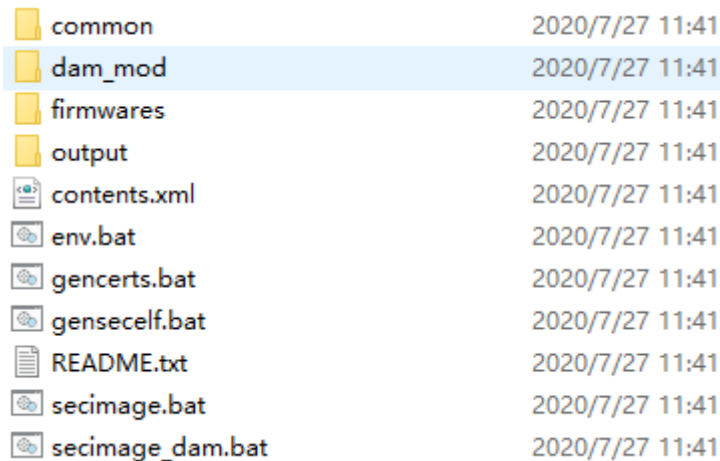
## 2.5. Hardware Foundation

The modules include one-time programmable fuses. The initial states of all fuses are 0 (Secure Boot disabled). Once a write operation is performed on the fuse (or the fuse is blown), the state of the fuse permanently becomes 1 (Secure Boot enabled). The state cannot be changed after the fuse is blown,

which means that the enablement of Secure Boot is an irreversible operation.

## 2.6. Secure Boot Toolkit

Quectel provides a Secure Boot toolkit (*Quectel SecBootTools*) to generate related certificates and the *sec.elf* file, and to sign software images.



common	2020/7/27 11:41
dam_mod	2020/7/27 11:41
firmwares	2020/7/27 11:41
output	2020/7/27 11:41
contents.xml	2020/7/27 11:41
env.bat	2020/7/27 11:41
gencerts.bat	2020/7/27 11:41
gensecelf.bat	2020/7/27 11:41
README.txt	2020/7/27 11:41
secimage.bat	2020/7/27 11:41
secimage_dam.bat	2020/7/27 11:41

**Figure 1: Quectel SecBootTools**

Functions of Quectel Secure Boot toolkit:

1. *gencerts.bat* generates the root certificate (*qpsa\_rootca.cer*) and the attestation certificate (*qpsa\_attestca.cer*) as well as the hash values.
2. *gensecelf.bat* generates *sec.elf*. See **Chapter 2.7** for details of *sec.elf*.
3. *secimage.bat* signs and re-signs the images (see **Chapter 2.4** for the list of images to be signed) including files in ELF/MBN format.
4. For details of the other files or folders in the toolkit, see *README.txt*.

### NOTE

Contact Quectel Technical Support ([support@quectel.com](mailto:support@quectel.com)) to acquire the Secure Boot toolkit.

## 2.7. sec.elf

The *sec.elf* file is vital for the enabling of Secure Boot, as it includes the configuration parameters for the function, as illustrated below.

1. Secure boot enabling
2. JTAG access disabling
3. Anti-rollback enabling
4. Read/Write permissions disabling/enabling for fuses
5. Fuse blowing

# 3 Enable Secure Boot

## 3.1. Procedure

### Step 1: Generate certificates and public key hash values

Run *gencerts.bat* in the Secure Boot toolkit to generate a root certificate and an attestation certificate, as well as a public key hash value of the root certificate. The generated certificates are used to sign images, and the hash value is used to verify the signed images. If any image does not pass verification, the loading of the image will fail.

Update the generated hash value to the *9205\_fuseblower\_USER.xml* file in the toolkit. For specific operations, see *README.txt* in the toolkit.

### Step 2: Generate sec.elf

Run *gensecelf.bat* in the toolkit to generate the *sec.elf* file. For details of *sec.elf*, see **Chapter 2.7**.

### Step 3: Sign images

Run *secimage.bat* in the toolkit to sign the necessary image files. For the list of necessary images, see **Chapter 2.4**.

### Step 4: Update firmware

Use the *sec.elf* and signed images generated in **Step 2** and **Step 3** to replace the ones in the original firmware package and then update the firmware. For details of how to update the firmware, see **document [1]**.

#### NOTE

After the Secure Boot is enabled, if you download an unsigned image, or use different certificates from the ones used for enabling Secure Boot to sign the image, the module will fail in downloading the firmware during firmware updating process.

## 3.2. Verification

After firmware updating, send **AT+QSECBOOTSTAT?** to query whether the module has enabled Secure Boot successfully.

### 3.2.1. AT+QSECBOOTSTAT? Query Secure Boot Status

This command queries the current status of Secure Boot.

AT+QSECBOOTSTAT? Query Secure Boot Status	
Read Command <b>AT+QSECBOOTSTAT?</b>	Response <b>+QSECBOOTSTAT: &lt;status&gt;</b>  <b>OK</b>  If there is any error related to ME functionality: <b>ERROR</b>
Maximum Response Time	300 ms

#### Parameter

<b>&lt;status&gt;</b>	Integer type. Secure Boot status. 0 Disabled 1 Enabled
-----------------------	--

#### Example

```

AT+QSECBOOTSTAT? //Query whether the module has enabled Secure Boot.
+QSECBOOTSTAT: 1 //The module has enabled Secure Boot.

OK

```

# 4 Appendix A References

**Table 2: Related Documents**

SN	Document Name	Description
[1]	Quectel_QFlash_User_Guide	User Guide of QFlash Tool
[2]	<i>PKCS #1</i>	RSA Cryptography Specifications
[3]	<i>ITU-T X.509</i>	Information technology – Open Systems Interconnection – The Directory: Public-key and attribute certificate frameworks

**Table 1: Terms and Abbreviations**

Abbreviation	Description
APPSBL	Applications Boot Loader
CA	Certificate Authority
ELF	Executable and Linkable Format
JATG	Joint Test Action Group (an industry standard for verifying designs and testing printed circuit boards)
PBL	Primary Boot Loader
PKCS	Public-Key Cryptography Standards
RoT	Root of Trust
RSA	Rivest–Shamir–Adleman
SBL	Secondary Boot Loader