

RG50xQ&RM5xxQ 系列

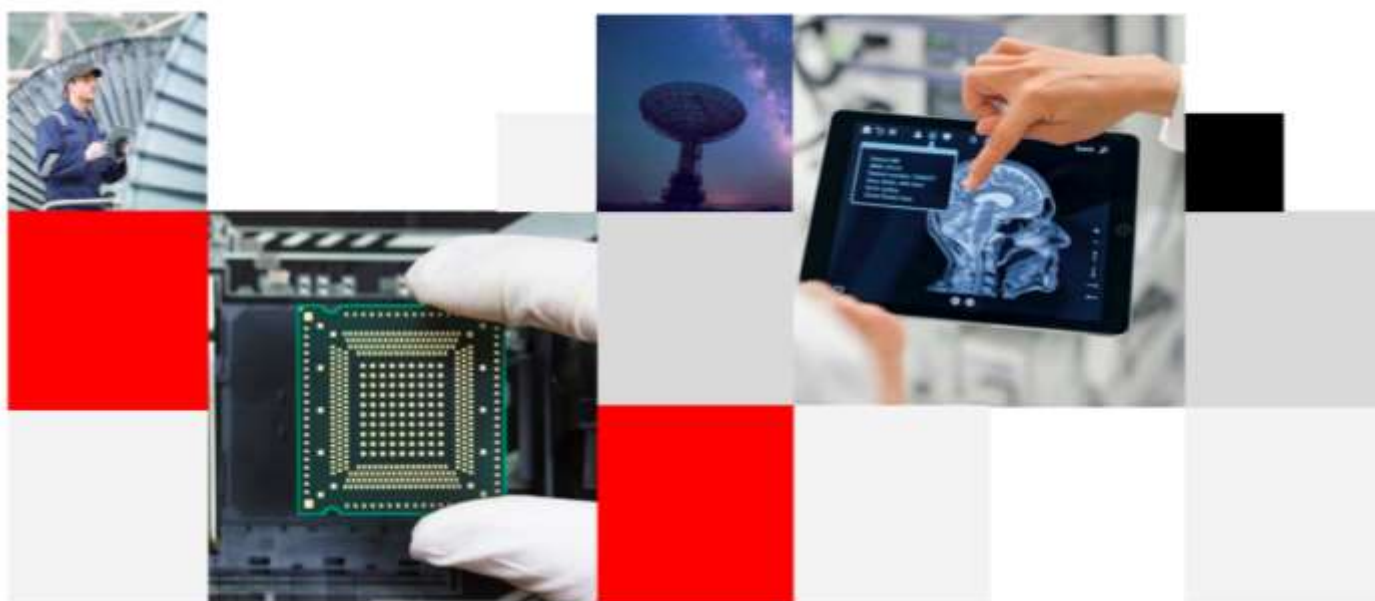
Secure Boot 应用指导

5G 模块系列

版本：1.0

日期：2021-04-02

状态：受控文件



Build a Smarter World

上海移远通信技术股份有限公司始终以为客户提供最及时、最全面的服务为宗旨。如需任何帮助，请随时联系我司上海总部，联系方式如下：

上海移远通信技术股份有限公司
上海市闵行区田林路 1016 号科技绿洲 3 期（B 区）5 号楼 邮编：200233
电话：+86 21 51086236 邮箱：info@quectel.com

或联系我司当地办事处，详情请登录：<http://www.quectel.com/cn/support/sales.htm>。

如需技术支持或反馈我司技术文档中的问题，可随时登陆如下网址：
<http://www.quectel.com/cn/support/technical.htm> 或发送邮件至：support@quectel.com。

前言

上海移远通信技术股份有限公司提供该文档内容用以支持其客户的产品设计。客户须按照文档中提供的规范、参数来设计其产品。因未能遵守有关操作或设计规范而造成的损害，上海移远通信技术股份有限公司不承担任何责任。在未声明前，上海移远通信技术股份有限公司有权对该文档进行更新。

免责声明

上海移远通信技术股份有限公司尽力确保开发中功能的完整性、准确性、及时性或效用，但不排除上述功能错误或遗漏的可能。除非其他有效协议另有规定，否则上海移远通信技术股份有限公司对开发中功能的使用不做任何暗示或明示的保证。在适用法律允许的最大范围内，上海移远通信技术股份有限公司不对任何因使用开发中功能而遭受的损失或损害承担责任，无论此类损失或损害是否可以预见。

保密义务

除非上海移远通信技术股份有限公司特别授权，否则我司所提供文档和信息的接收方须对接收的文档和信息保密，不得将其用于除本项目的实施与开展以外的任何其他目的。未经上海移远通信技术股份有限公司书面同意，不得获取、使用或向第三方泄露我司所提供的文档和信息。对于任何违反保密义务、未经授权使用或以其他非法形式恶意使用所述文档和信息的违法侵权行为，上海移远通信技术股份有限公司有权追究法律责任。

版权申明

本文档版权属于上海移远通信技术股份有限公司，任何人未经我司允许而复制转载该文档将承担法律责任。

版权所有 ©上海移远通信技术股份有限公司 2021，保留一切权利。

Copyright © Quectel Wireless Solutions Co., Ltd. 2021.

文档历史

修订记录

版本	日期	作者	修改描述
-	2021-03-22	Ritchie WU	文档创建
1.0	2021-04-02	Ritchie WU	受控版本

目录

文档历史	3
目录	4
表格索引	5
1 引言	6
1.1. 适用模块	6
2 Secure Boot 概述	7
2.1. Secure Boot 定义	7
2.2. 使能 Secure Boot	7
2.3. 证书链	7
2.4. 签名镜像文件	8
2.5. QFPROM 配置	8
3 Secure Boot 相关 AT 命令	9
3.1. AT 命令语句	9
3.1.1. 定义	9
3.1.2. AT 命令语句	9
3.2. AT 示例声明	10
3.3. AT 命令详解	10
3.3.1. AT+QSECBOOT 使能或查询 Secure Boot 功能	10
3.3.1.1. AT+QSECBOOT="status" 查询 Secure Boot 使能状态	10
3.3.1.2. AT+QSECBOOT="serialnum" 查询模块唯一序列号	11
3.3.1.3. AT+QSECBOOT="progsec" 使能 Secure Boot 功能	11
4 注意事项	13
5 附录 A 术语缩写	14

表格索引

表 1: 适用模块	6
表 2: AT 命令类型	9
表 3: 术语缩写	14

1 引言

移远通信 5GRG50xQ 系列和 RM50xQ 系列模块支持 Secure Boot 功能。本文档介绍如何使用 AT 命令在 RG50xQ 系列和 RM50xQ 系列模块上开启 Secure Boot 功能，包括 Secure Boot 概述、AT 命令详解以及注意事项。

1.1. 适用模块

表 1：适用模块

模块系列	模块
RG50xQ	RG500Q系列
	RG501Q-EU
	RG502Q-EA
RM50xQ	RM500Q系列
	RM502Q系列
	RM505Q-AE
	RM510Q-GL

2 Secure Boot 概述

2.1. Secure Boot 定义

Secure Boot 是一种建立在授信平台上的安全启动序列。为了保证仅执行通过验证的软件，Secure Boot 在启动过程中增加了验证签名环节。

为防止没有经过合法签名或被恶意修改的软件在模块上运行，Secure Boot 在模块启动过程的每个阶段均增加了验证签名环节。在一系列启动阶段中，需有一个根信任实体，RG50xQ 和 RM5xxQ 系列模块中的 PBL 作为固件固化在模块中，且无法被修改，可作为根信任实体。

2.2. 使能 Secure Boot

仅可通过硬件上的熔断器使能 Secure Boot，且使能后无法关闭 Secure Boot。

模块的启动过程分为多个阶段，每个阶段都由一个专用的镜像文件完成特定的功能。使能 Secure Boot 之后，每一阶段的镜像文件在执行前，都需要前一阶段的镜像文件对其进行校验；如果校验失败，会造成整个启动过程失败，进而模块启动失败。

作为信任根，PBL（也称为 RoT）是一种包含在芯片中的固件且无法修改，因此是可信任的（启动过程的最信任实体）并可作为下一启动阶段的授信中心；下一启动阶段一般是 SBL 经过验证签名后被执行，后续的启动阶段都可以使用 SBL 进行授信操作。

2.3. 证书链

Secure Boot 支持 2048 位或 4096 位的 RSA 秘钥，用于证书以及镜像文件的签名。证书签名支持的格式为 PKCS v1.2 标准格式，支持 SHA-256 算法或 SHA-384 算法。

模块的证书链支持两级证书或者三级证书，默认采用两级的证书链：Self-signed root certificate 和 Attestation certificate。

2.4. 签名镜像文件

镜像文件的标准格式为 ELF，在 Secure Boot 中，验证启动过程中的每个阶段需要对每个阶段的镜像文件进行签名操作。标准的 ELF 格式二进制文件包含多个段，分别代表不同种类的信息，其中签名相关的信息保存在 *Hash table segment* 中。*Hash table segment* 中还包含每个段的 hash 值，以及证书信任链相关的信息。

模块中必须签名的镜像文件如下：

- *abl.elf*
- *aop.mbn*
- *devcfg.mbn*
- *hyp.mbn*
- *multi_image.mbn*
- *prog_firehose_sdx55.mbn*
- *sbl1.mbn*
- *tz.mbn*
- *uefi.elf*
- *xbl_cfg.elf*
- *apdp.mbn*
- *NON-HLOS.ubi*

2.5. QFPROM 配置

RG50xQ 和 RM5xxQ 系列模块包含一次性可编程熔断器。所有熔断器初始状态均为 0（表示未启动 Secure Boot）。一旦进行写入（或者熔断）操作，熔断器状态将永久地改变为 1（表示启动 Secure Boot）。熔断后，状态无法改变。需要使用 QFPROM 编程工具协助完成 Secure Boot 的启动。

QFPROM 用于在一个非易失性 ROM（non-volatile read-only memory）中存储代表芯片鉴权相关的配置，可实现 Secure Boot 所需的安全环境。配置 QFPROM，进行熔断操作，进而完成所需要的安全功能，例如：Debug 端口的输出功能、JTAG 功能、安全文件系统和软件回滚功能等。

3 Secure Boot 相关 AT 命令

3.1. AT 命令语句

3.1.1. 定义

- **<CR>** 回车符。
- **<LF>** 换行符。
- **<...>** 参数名称。实际命令行中不包含尖括号。
- **[...]** 可选参数或 TA 信息响应的可选部分。实际命令行中不包含方括号。若无特别说明，配置命令中的可选参数被省略时，将默认使用其之前已设置的值或其默认值。
- **下划线** 参数的默认设置。

3.1.2. AT 命令语句

前缀 **AT** 或 **at** 必须加在每个命令行的开头。输入 **<CR>** 将终止命令行。通常，命令后面跟随形式为 **<CR><LF><response><CR><LF>** 的响应。在本文档中，仅显示响应 **<response>**，省略 **<CR><LF>**。

表 2: AT 命令类型

AT 命令类型	语句	描述
测试命令	AT+<cmd>=?	测试是否存在相应的设置命令，并返回有关其参数的类型、值或范围的信息。
查询命令	AT+<cmd>?	查询相应设置命令的当前参数值。
设置命令	AT+<cmd>=<p1>[,<p2>[,<p3>[...]]]	设置用户可定义的参数值。
执行命令	AT+<cmd>	返回特定的参数信息或执行特定的操作。

3.2. AT 示例声明

本文中的示例仅为方便用户了解 AT 命令的使用方法，不构成移远通信对终端流程设计的建议或意见，也不代表模块应被设置成相应示例中的状态。某些 AT 命令存在多个示例，这些示例之间不存在承接关系或连续性。

3.3. AT 命令详解

3.3.1. AT+QSECBOOT 使能或查询 Secure Boot 功能

AT+QSECBOOT 使能或查询 Secure Boot 功能	
测试命令 AT+QSECBOOT=?	响应 +QSECBOOT: "status", (支持的<enable>列表) +QSECBOOT: "serialnum", <serial_number> +QSECBOOT: "progsec", (支持的<enable>列表) OK 或者 ERROR
最大响应时间	300 毫秒
特性说明	/

3.3.1.1. AT+QSECBOOT="status" 查询 Secure Boot 使能状态

该命令用于查询模块当前是否已使能 Secure Boot 功能。

AT+QSECBOOT="status" 查询 Secure Boot 使能状态	
设置命令 AT+QSECBOOT="status"	响应 +QSECBOOT: "status", <enable> OK 或者 ERROR
最大响应时间	300 毫秒
特性说明	/

参数

<enable>	整型。Secure Boot 功能使能状态。
1	Secure Boot 已被使能
0	Secure Boot 未被使能

3.3.1.2. AT+QSECBOOT="serialnum" 查询模块唯一序列号

该命令用于查询模块的唯一序列号。

AT+QSECBOOT="serialnum" 查询模块唯一序列号

设置命令 AT+QSECBOOT="serialnum"	响应 +QSECBOOT: "serialnum",<serial_number> OK 或者 ERROR
最大响应时间	300 毫秒
特性说明	/

参数

<serial_number>	字符串类型。模块的序列号。十六进制格式，不含双引号。
------------------------------	----------------------------

3.3.1.3. AT+QSECBOOT="progsec" 使能 Secure Boot 功能

该命令用于使能 Secure Boot 功能。

AT+QSECBOOT="progsec" 使能 Secure Boot 功能

设置命令 AT+QSECBOOT="progsec",<enable>	响应 若省略可选参数，则查询当前状态： +QSECBOOT: "progsec",<enable> OK 若指定可选参数，则使能 Secure Boot 功能： OK 或者
---	---

	ERROR
最大响应时间	300 毫秒
特性说明	该命令立即生效。

参数

<enable>	整型。使能 Secure Boot 功能。
	1 使能 Secure Boot
	0 未使能 Secure Boot（仅在查询结果中有效）

4 注意事项

1. Secure Boot 功能只能通过硬件上的 Fuse 打开，一旦打开无法关闭。
2. 推荐使用 **AT+QSECBOOT="progsec",<enable>**使能 Secure Boot 功能，模块中 Secure Boot 功能默认未使能；该命令在 **sec** 分区中烧录镜像文件，重启模块后自动激活 Secure Boot 功能。使能 Secure Boot 功能后无法通过 Firehose 将固件降级到不支持 Secure Boot 功能的版本。
3. 使能 Secure Boot 功能后，不支持通过 DFOTA 将版本降级至不支持 Secure Boot 功能的固件版本，否则将导致无法正常启动模块。
4. PCIe Fuse 模式也是在 **sec** 分区中烧录镜像文件，与 Secure Boot 的使能有冲突。若先使能 Secure Boot 功能，则无法使能 PCIe Fuse 模式。因此建议使能 PCIe Fuse 模式后再使能模块的 Secure Boot 功能。

5 附录 A 术语缩写

表 3：术语缩写

缩写	英文全称	中文全称
DFOTA	Delta Firmware Upgrade Over-The-Air	固件空中差分升级
ELF	Executable and Linkable Format	可执行可链接格式
MBN	Multi Boot Image Format	多启动镜像文件格式
PBL	Primary Boot Loader	主引导加载程序
PCIe	Peripheral Component Interconnect Express	快捷外围部件互连标准
PKCS	Public-Key Cryptography Standards	公钥密码学标准
QFPROM	Qualcomm Fuse Programmable Read Only Memory	一次性可编程只读存储器
RPM	RPM Package Manager (originally Red Hat Package Manager)	RPM软件包管理器
RoT	Root of Trust	可信根
SBL	Secondary Boot Loader	二级引导加载程序
SHA	Secure Hash Algorithm	安全散列算法