AirPrime HL78xx Secure Boot

2174239-1

Author:	Sierra Wireless	Date:	November 15, 2020

APN Content Level	BASIC	✓	INTERMEDIATE		ADVANCED		Confidentiality	Public		Private	✓

Hardware Compatibility	Product Line	AirPrime	Series	HL78xx	

Software Compatibility	Firmware	ALL	Document Type	Application Note	✓	Technical Note	

1 Version

This document may be updated over its lifetime. To ensure you design with the correct version, please check The Source page on www.sierrawireless.com for the latest version.

2 Introduction

This document is provided to Sierra Wireless distributors and clients to aid more rapid development of embedded applications using the Sierra Wireless portfolio of cellular solutions. To request a new application/technical note, contact your regional Sierra Wireless Product Marketing Manager.

3 Glossary

Term/Initials	Definition
App FW	Application Firmware
BootROM	ROM bootloader
FOTA	Firmware update Over The Air
FW	Firmware
HSM	Hardware Secure Module
Modem FW	Cat-M1 modem image
Modem FW2	NB1 modem image
OTP	One Time Programmable memory
PrK	Private Key
PuK	Public Key
U-Boot	Universal Boot Loader

4 Overview

This document describes the Secure Boot mechanism on AirPrime HL78xx modules, and related Sierra Wireless processes used to deploy the Secure Boot feature.

The secure boot feature is used to protect the FW from hacking. If the module is secured, only signed images can be run (unsigned images will fail). The feature uses a chained approach to authenticate the images through the whole boot chain. The BootROM authenticates the U-Boot image against a digital signature before being executed. U-boot then authenticates other images.

5 Secure Boot Mechanism

5.1 Secure Boot Process

Secure boot refers to the boot sequence that establishes a trusted platform for secure applications. Secure boot starts as an immutable sequence that validates the origin of the code using cryptographic authentication, so only authorized software can be executed. The boot sequence places the device in a known security state and protects against binary manipulation of software and re-flashing attacks.

5.1.1 Secure Boot Sequence

The HL78xx boot sequence starts with the BootROM, a static piece of software stored in the chipset that cannot be altered. The BootROM then starts the bootloader (i.e. U-Boot for HL78xx) which, in turn, starts the relevant firmware (modem and application firmware).

A secure boot sequence adds an authentication stage where each element of the sequence authenticates the next one before it runs – the BootROM authenticates the bootloader, and the bootloader authenticates the firmware package. See Figure 1 below for the boot-up trusted sequence.

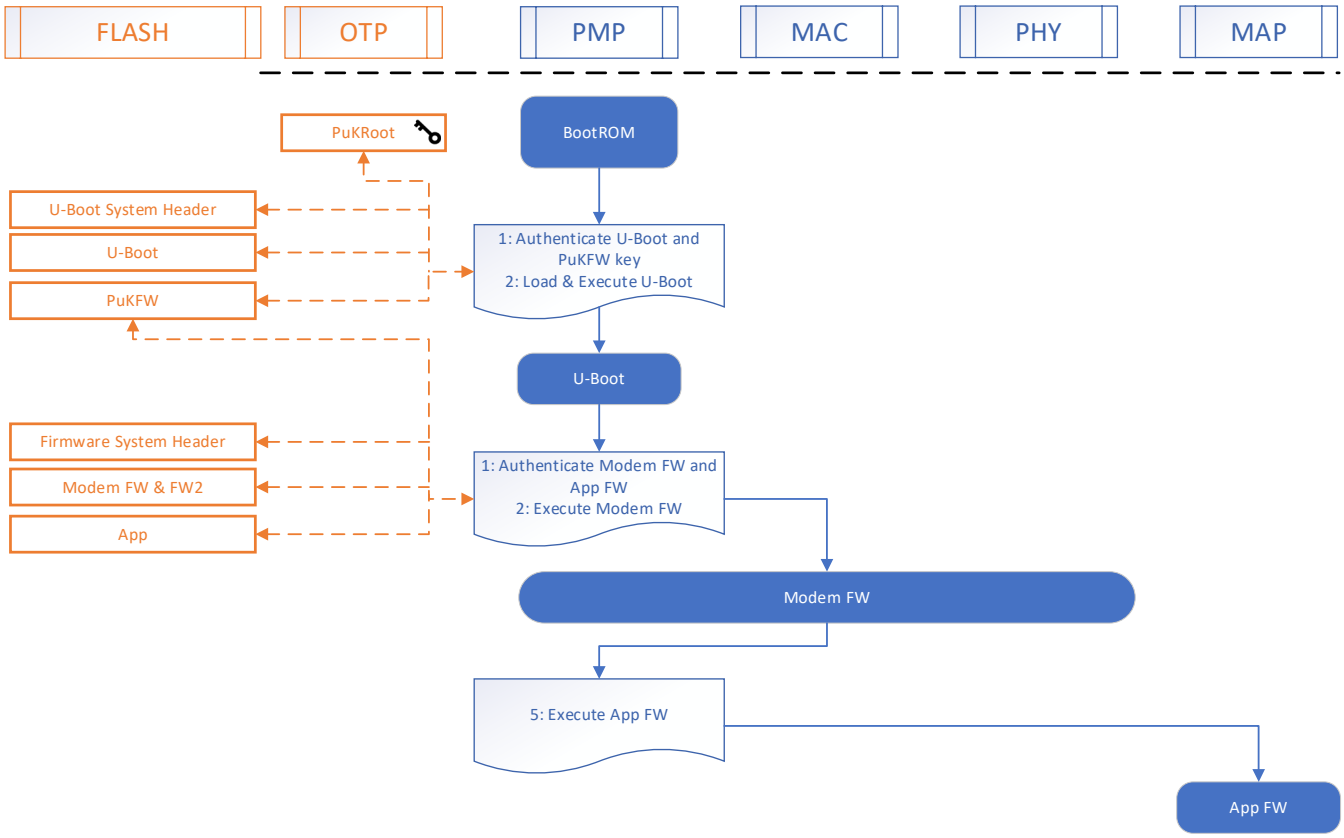

Figure 1. Secure Boot Architecture

The boot sequence steps are:

1. BootROM authenticates the U-Boot package (U-Boot image and the public key used to authenticate other firmware images.)
2. BootROM loads and executes U-Boot.
3. U-Boot authenticates modem FW & FW2 and App FW.
4. U-Boot executes modem FW or modem FW2 according to the selected RAT
5. Modem FWx executes App FW.

This boot sequence applies at each cold boot, or after a soft or hard reset.

5.1.2 Signed Package Format

Each image is associated with an image header. This image header contains information such as the size, image start address and the image hash.

A System Header is a collection of image headers plus a digital signature that is calculated over these image headers.

A Signed Package is composed of a System Header and its associated images (Figure 2 below).

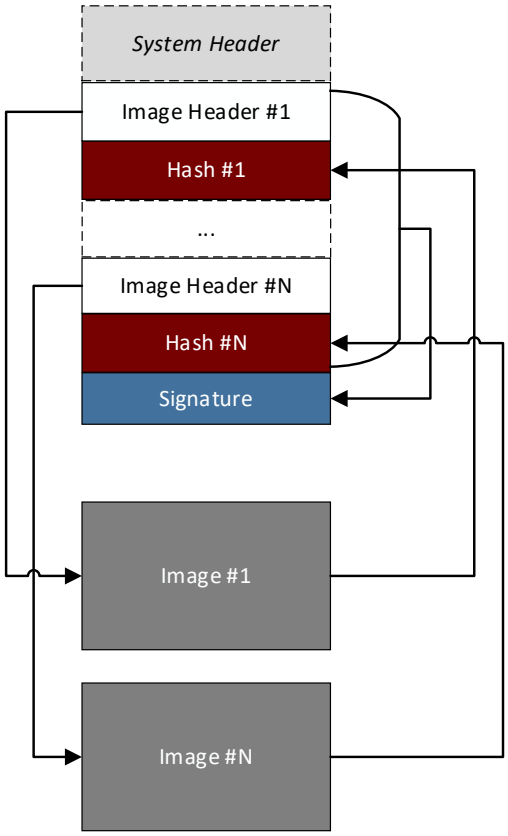

Figure 2. Signed Package Format

For the AirPrime HL78xx module, there are two signed packages:

- U-Boot signed package containing:
  - System header
  - U-Boot image
  - PuKFw key image
- Firmware signed package
  - System header
  - Modem FW image
  - Modem FW2 image
  - Application image

5.2 Digital Signatures & Key Storage

5.2.1 ECDSA Signature

The U-Boot package is signed using an elliptic curved digital signature algorithm (ECDSA). This algorithm combines small key sizes and a high level of security. Key size is important here as the U-Boot authenticating Public Key (PuKRoot) will be stored in OTP (One Time Programmable) memory.

The U-Boot package is authenticated via an ECC P-256 digital signature.

5.2.2 RSA Signature

An RSA key pair will be used to sign and authenticate the firmware package. The public key (PuKFw) will be stored in flash memory where storage constraints are fewer than in OTP memory. The use of RSA instead of ECDSA is driven by performance concerns – authentication challenge is much quicker to perform using RSA.

The Firmware package is authenticated via an RSA-3072 digital signature.

5.2.3 Key Storage

Private keys (PrKRoot and PrKFw) are stored securely in an HSM. Only Sierra Wireless security officers can sign a U-Boot or firmware package.

Public keys are stored locally in the device at the production stage:

- PuKRoot is stored in OTP memory.
- PuKFw is stored in flash memory and authenticated within the U-Boot package with PuKRoot.

5.3 Anti-Rollback Mechanism

The anti-rollback mechanism is used to prevent version downgrade in case a security vulnerability is present on the previous U-Boot or firmware package version.

A rollback counter is included in the U-Boot package system header. The rollback counter is checked against an OTP field. If the U-Boot package rollback counter is greater than the OTP rollback counter, the OTP rollback counter is updated with this U-Boot package rollback counter.

When the module is powered on, U-Boot is executed only if the U-Boot package rollback counter is equal to or greater than the OTP rollback counter.

The same anti-rollback mechanism applies on the firmware package. It is based on a rollback counter included in the firmware package system header and a dedicated OTP counter.

U-Boot and firmware packages' rollback counters can then be updated independently.

6 Secured HL78xx AirPrime Module Identification

The ATI9 command has been extended to provide new device security-related information.

For example (refer to [1] AirPrime HL78xx AT Commands Interface Guide for additional details):

```
ATI9
<modem SW version>
<Long revision identification>
<Build Date and Time>
IMEI-SV:<IMEI-SV version>
Legato RTOS: <Legato RTOS version and binary date>
<Component>: <Component version>
...
SBUB: <SBUB>
SBFW: <SBFW>
RPuK: <RPuK>
FPuK: <FPuK>
RBUB: <RBUB>
RBFW: <RBFW>

OK
```

New components are introduced to identify a device that has secure boot activated. CRC32 checksums of the installed RPuK and FPuK public keys are displayed as well as the roll back status. These new components are the following:

- <SBUB>– Secure boot activation status for the bootloader
  - 0 – Not activated
  - 1 - Activated
- <SBFW>– Secure boot activation status for the firmware package
  - 0 – Not activated
  - 1 - Activated

- <RPuK> – CRC32 checksum of the root public key in OTP (empty if secure boot is not active for the bootloader), displayed in hexadecimal.
- <FPuK> – CRC32 checksum of the firmware package public key (empty if secure boot is not active for the firmware package), displayed in hexadecimal.
- <RBUB>– Anti-rollback counter for the bootloader image, displayed in decimal
- <RBFW>– Anti-rollback counter for the modem package, displayed in decimal

The new components are also displayed for non-secured devices, with the following differences:

- RPuK shows no value when secure boot is not activated (i.e. when SBUB shows 0)
- FPuK shows no value when secure boot is not activated (i.e. when SBFW shows 0)

Example:

- Secure boot enabled device:

```
SBUB: 1          ← New component
SBFW: 1          ← New component
RPuK: 53F7A48A   ← New component
FPuK: 139A8E70   ← New component
RBUB: 0
RBFW: 0
```

- Non-secured device:

```
SBUB: 0          ← New component
SBFW: 0          ← New component
RPuK:            ← New component
FPuK:            ← New component
RBUB: 0
RBFW: 0
```

7 Package Signature

7.1 Package Signature Generation

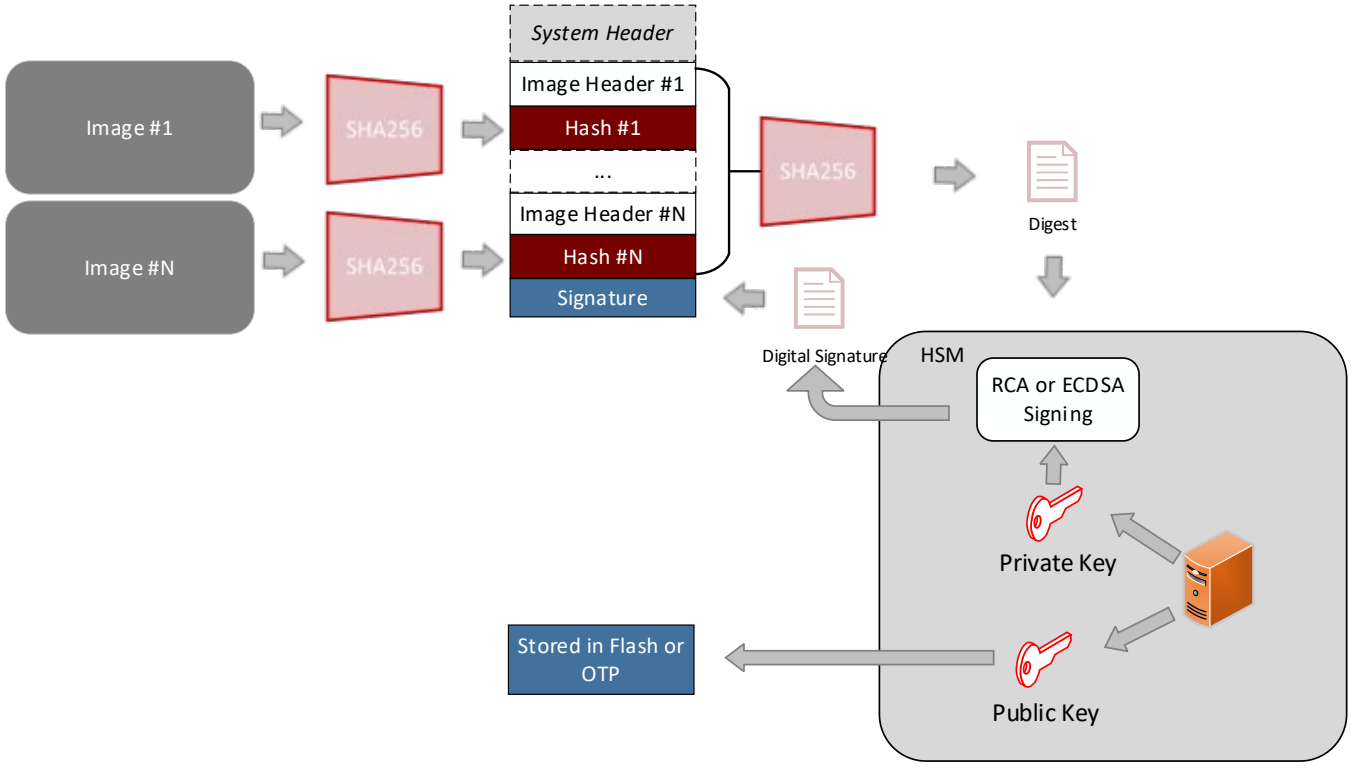

Figure 3. Package Signature Generation

The logic behind the signing of the U-Boot and firmware packages is similar except for the signing algorithm itself – ECDSA for the U-Boot package, and RSA for the firmware package.

A SHA-256 hash is generated over the data to sign. The hash value is signed using ECDSA or RSA and the relevant private key (PrKRoot for U-Boot package, PrKFw for the firmware package). The resulting signature is appended to the System Header of the package.

7.2 Package Signature Verification

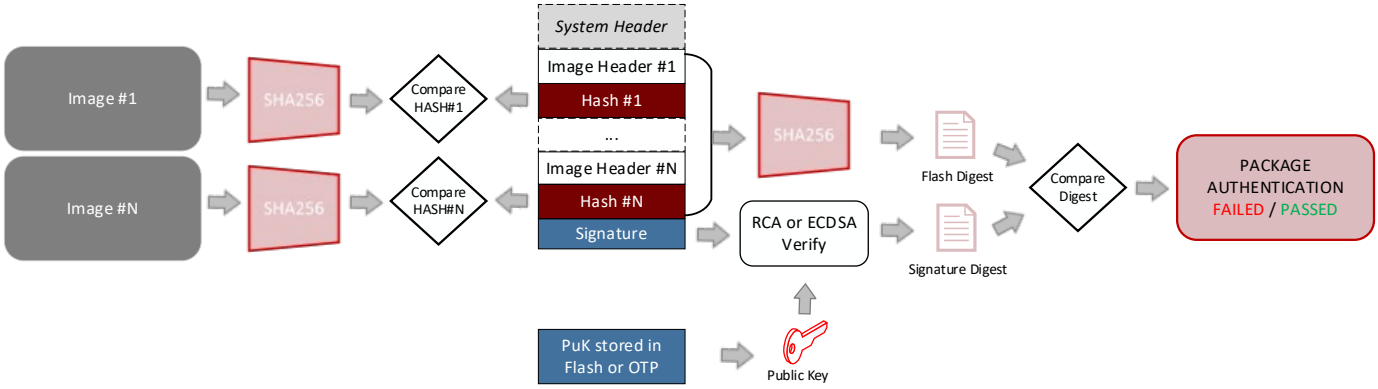

Figure 4. Package Signature Verification

Package signature verification is done according to Figure 4 above.

For each image identified into the signed package, a SHA-256 image hash is computed and compared to the hash present in the package system image header.

If all hashes match, package verification continues with the signature verification. If the digest calculated from the RSA or ECDSA verification and the digest calculated over the package system header match, authentication is successful. Otherwise it is considered as failed.

8 Signed Package Release Process

U-Boot and Firmware packages are generated using the same process for secure and non-secure AirPrime HL78xx modules.

These packages are first signed with an engineering key and can run on non-secure modules or secure engineering modules. Engineering modules are provisioned with engineering keys and are only used by Sierra Wireless for its own development and validation tasks.

Once the packages are validated and meet Sierra Wireless' quality and security criteria, the packages are then signed by the Security officers using the production key stored in the HSM as described in **7.1 Package Signature Generation**.

Such packages signed with production keys can be executed on non-secure modules, or secure modules provisioned with the production key. Some validation tests (mainly FOTA regression tests) are performed before the signed packages are officially released.

Figure 5. Signed Package Release Process

Signed packages are delivered in the same format as unsigned packages:

- Windows One-click exe
- Zip file containing signed packages + sft tool for Windows and Linux
- Delta FOTA packages

9 Reference Documents

	Filename	Document number
[1]	AirPrime HL78xx AT Commands Interface Guide	41111821
[2]	AirPrime HL78xx Product Technical Specification	41113770

10 Support

For direct clients: contact your Sierra Wireless FAE

For distributor clients: contact your distributor FAE

For distributors: contact your Sierra Wireless FAE

11 Document History

Level	Date	History
0.1	November 29, 2018	Creation
0.2	January 8, 2019	Minor Updates
1	December 3, 2020	General release – Minor updates, added HL7802

12 Legal Notice

Sierra Wireless modem in any aircraft, whether the aircraft is on the ground or in flight. In aircraft, the Sierra Wireless modem **MUST BE POWERED OFF**. When operating, the Sierra Wireless modem can transmit signals that could interfere with various onboard systems.

Note: Some airlines may permit the use of cellular phones while the aircraft is on the ground and the door is open. Sierra Wireless modems may be used at this time.

The driver or operator of any vehicle should not operate the Sierra Wireless modem while in control of a vehicle. Doing so will detract from the driver or operator's control and operation of that vehicle. In some states and provinces, operating such communications devices while in control of a vehicle is an offence.

Limitations of Liability

This manual is provided "as is". Sierra Wireless makes no warranties of any kind, either expressed or implied, including any implied warranties of merchantability, fitness for a particular purpose, or noninfringement. The recipient of the manual shall endorse all risks arising from its use.

The information in this manual is subject to change without notice and does not represent a commitment on the part of Sierra Wireless. SIERRA WIRELESS AND ITS AFFILIATES SPECIFICALLY DISCLAIM LIABILITY FOR ANY AND ALL DIRECT, INDIRECT, SPECIAL, GENERAL, INCIDENTAL, CONSEQUENTIAL, PUNITIVE OR EXEMPLARY DAMAGES INCLUDING, BUT NOT LIMITED TO, LOSS OF PROFITS OR REVENUE OR ANTICIPATED PROFITS OR REVENUE ARISING OUT OF THE USE OR INABILITY TO USE ANY SIERRA WIRELESS PRODUCT, EVEN IF SIERRA WIRELESS AND/OR ITS AFFILIATES HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES OR THEY ARE FORESEEABLE OR FOR CLAIMS BY ANY THIRD PARTY.

Notwithstanding the foregoing, in no event shall Sierra Wireless and/or its affiliates aggregate liability arising under or in connection with the Sierra Wireless product, regardless of the number of events, occurrences, or claims giving rise to liability, be in excess of the price paid by the purchaser for the Sierra Wireless product.

Patents

This product may contain technology developed by or for Sierra Wireless Inc.

This product includes technology licensed from QUALCOMM®.

This product is manufactured or sold by Sierra Wireless Inc. or its affiliates under one or more patents licensed from MMP Portfolio Licensing.

Copyright

Trademarks

Sierra Wireless®, AirPrime®, AirLink®, AirVantage®, WISMO®, ALEOS® and the Sierra Wireless and Open AT logos are registered trademarks of Sierra Wireless, Inc. or one of its subsidiaries.

Watcher® is a registered trademark of NETGEAR, Inc., used under license.

Windows® and Windows Vista® are registered trademarks of Microsoft Corporation.

Macintosh® and Mac OS X® are registered trademarks of Apple Inc., registered in the U.S. and other countries.

QUALCOMM® is a registered trademark of QUALCOMM Incorporated. Used under license.

Other trademarks are the property of their respective owners.