Apacer

Signed Firmware

White Paper

March 5, 2021

Version 1.2

Apacer Technology Inc.
1F, No.32, Zhongcheng Rd., Tucheng Dist., New Taipei City, Taiwan, R.O.C
Tel: +886-2-2267-8000 Fax: +886-2-2267-2261
www.apacer.com

Table of Contents

1. Introduction

Updating a piece of software or firmware is no longer the simple process it was 10 or 20 years ago. In the modern world, downloading software, firmware, or any other file can be a vector for hackers to deliver malware, Trojans or worse. That's why Apacer developed a Signed Firmware method for delivering safe, authorized firmware updates that users will never need to worry about. This method relies on the well-established asymmetric encryption process to keep things secure.

This white paper will outline the methods Apacer uses to protect its downloadable firmware updates, and the process for users to safely access firmware updates online.

2. Keeping Firmware Secure

Before diving into the mechanics of updating firmware, it's important to understand how SSDs keep firmware secure in the first place.

2.1 Creating Signed Firmware

The process begins when an SSD manufacturer, such as Apacer, creates the firmware for an SSD under development. This firmware will be encrypted using a private key, generated by the SSD manufacturer. From this key, a public key will also be created which is a cryptographic 'match' for the private key. The firmware is considered "signed" if both a public key and a private key are required for it to run on the SSD. This process is illustrated in Figure 1, below.

When firmware updates are released in the future, they will also need to be signed if they are expected to run on the same SSD.

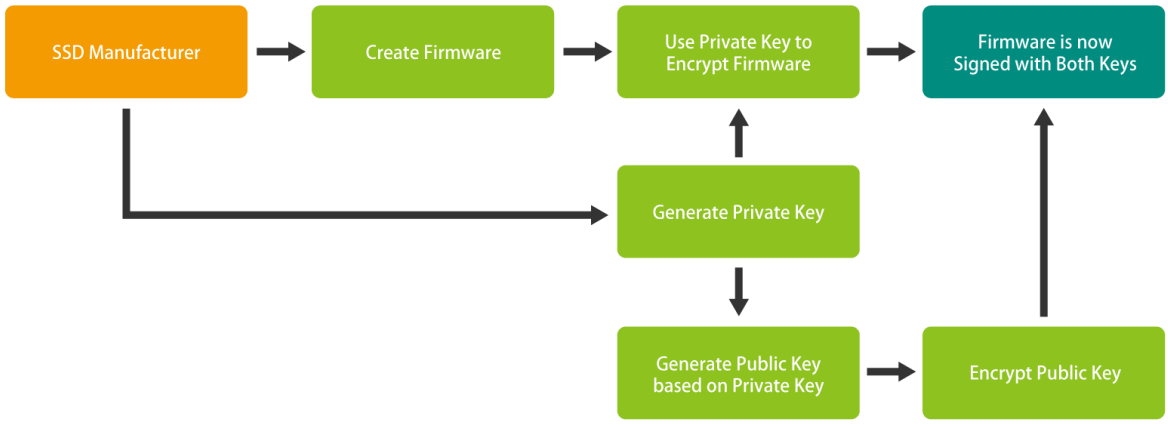

Figure 1: Process for Keeping an SSD's Firmware Secure

Once the raw firmware data is encrypted with the public key, it is totally secure. It can only be unlocked and installed on the SSD by the SSD manufacturer.

This method provides a level of security over and above what most SSDs can offer. Consequently, SSD buyers who require the highest levels of protection in their systems are encouraged to choose this firmware encryption technology. This technology predates the concept of signed firmware updates, and signed firmware updating only really applies to SSDs protected by this technology.

2.2 The Secure Boot Process

The secure boot process will take place every time the SSD with Signed Firmware is turned on. This is a rather simple, but highly secure process. After the SSD is powered on, it will compare the public key to the Signed Firmware to ensure that they match. If they don't, the drive will enter "Recovery Mode," and the data saved on the drive will be inaccessible to the user (although it remains intact on the drive itself). If they do match, the drive will boot normally and the user will be able to read saved data and write new data as one would normally expect. This process is illustrated in Figure 2 below.

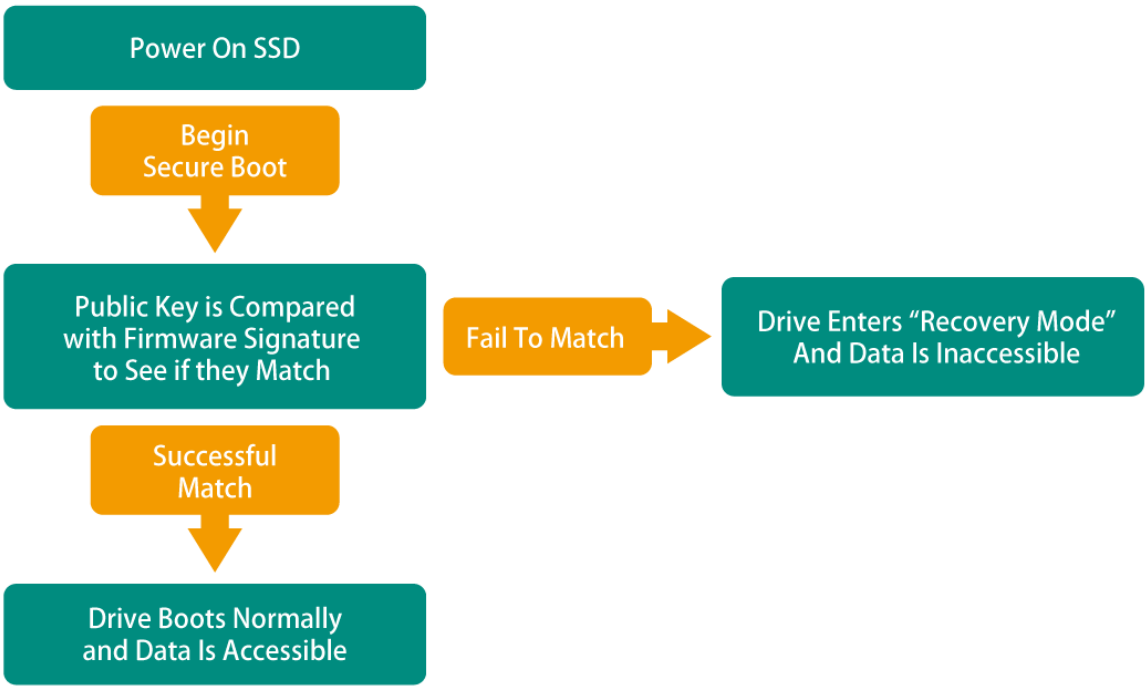

Figure 2: The Secure Boot Process

3. Updating A Drive's Firmware

3.1 Ensuring The Firmware Is Suitable

In most situations, an update to a drive's firmware will not be a common occurrence. However, when it is necessary to carry such an operation out, the user must take care to ensure that the firmware is updated in a secure way.

In particular, the user should pay attention to three crucial details. First of all, the code must be genuine code supplied by Apacer and it must be verified with the correct public key. Second of all, the code has the correct security information and is compatible with the drive in question. Finally, the new code is chronologically compatible with the old code.

If all three conditions are satisfied, the firmware can be safely updated.

3.2 Compatibility

Only certain versions of Apacer drives are compatible with the signed firmware protocol. If a user wishes to enquire about whether or not a particular drive is compatible with this protocol, they should contact a sales representative.

3.3 The Updating Process

The process of a signed firmware update is as follows.

First, the Apacer firmware team creates a firmware bin file, after extensive testing at our factory in Taipei. At this time, the firmware file is packaged with a public key. This will allow for verification of the firmware by the drive in the future. Once the firmware download file is virtually packaged in this way, it is made available to our users.

When a user wishes to update the firmware on their Apacer drive, they download the firmware bin file. First, the drive will validate the public key that is part of the package. If it fails to validate properly for

some reason, the update process will be halted. If, instead, the public key is valid, the drive will proceed to unpack the firmware. Then, after a further check to ensure the new firmware is compatible with the drive in question, the drive will carry out the firmware updating process, which may take a few minutes.

The process is illustrated in Figure 3 below. Please note that this is only a rough example.

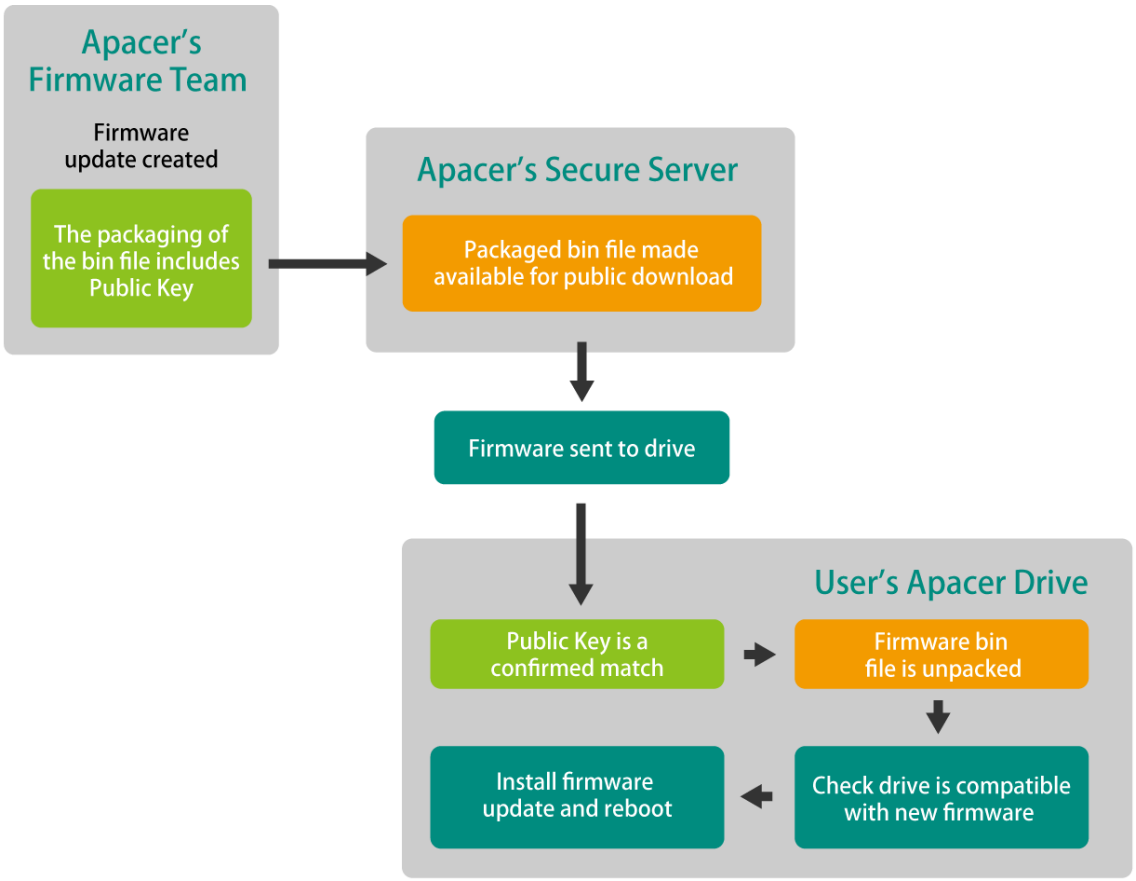

Figure 3: Process for Receiving, Confirming and Installing Signed Firmware

3. Conclusion

Apacer's signed firmware technology is a simple and reliable way for users to be sure that their Apacer drives only install valid and authentic firmware created by Apacer's professional firmware team. The process of downloading signed firmware generally happens without the user noticing what's going on in the drive, but it's important for all users to know that their firmware update is as secure as any other component in the drive production and maintenance process.

Revision History

Revision	Description	Date
1.0	Official release	12/14/2020
1.1	Updated charts and added Secure Boot.	1/6/2021
1.2	Updated small amount of text in charts	3/5/2021

Global Presence

Taiwan (Headquarters)
Apacer Technology Inc.
1F., No.32, Zhongcheng Rd., Tucheng Dist.,
New Taipei City 236, Taiwan R.O.C.
Tel: 886-2-2267-8000
Fax: 886-2-2267-2261
amtsales@apacer.com

U.S.A.
Apacer Memory America, Inc.
46732 Lakeview Blvd., Fremont, CA 94538
Tel: 1-408-518-8699
Fax: 1-510-249-9551
sa@apacerus.com

Japan
Apacer Technology Corp.
6F, Daiyontamachi Bldg., 2-17-12, Shibaura, Minato-Ku,
Tokyo, 108-0023, Japan
Tel: 81-3-5419-2668
Fax: 81-3-5419-0018
jpservices@apacer.com

Europe
Apacer Technology B.V.
Science Park Eindhoven 5051 5692 EB Son,
The Netherlands
Tel: 31-40-267-0000
Fax: 31-40-290-0686
sales@apacer.nl

China
Apacer Electronic (Shanghai) Co., Ltd
Room D, 22/FL, No.2, Lane 600, JieyunPlaza,
Tianshan RD, Shanghai, 200051, China
Tel: 86-21-6228-9939
Fax: 86-21-6228-9936
sales@apacer.com.cn

India
Apacer Technologies Pvt Ltd,
1874, South End C Cross, 9th Block Jayanagar,
Bangalore-560069, India
Tel: 91-80-4152-9061/62
Fax: 91-80-4170-0215
sales_india@apacer.com