RTD Embedded Technologies, Inc: TPM 1.2 to 2.0 Migration Guide

Note

This guide is written for individuals with knowledge of Bay Trail CPU modules and TPM 1.2 functionality to provide a high-level step by step checklist to upgrade to TPM 2.0. If you require additional information, please reference RTD's TPM Implementation User's Manual to learn about TPM 1.2 and/or 2.0 software and hardware in much finer detail.

Reasons for Upgrading from TPM 1.2 to TPM 2.0

In 2017 a new algorithm, named Return of Coppersmith's Attack (ROCA) was discovered. The algorithm used the public half of the RSA key to predict the private half of the RSA key. This is not a problem for TPM 2.0 chips using AES encryptions, but for older TPM 1.2 chips and USB smart cards which are limited to RSA keys and therefore vulnerable to ROCA. The currently accepted fix is to use RSA key lengths that have been shown to be less susceptible to ROCA, which include 1952-bit, 3072-bit, and 3936-bit. The best solution, however, is to upgrade to TPM 2.0 AES encryption hardware wherever possible.

Other TPM 2.0 Improvements

- TPM 2.0 chips support both RSA and AES keys as well as SHA-1, SHA-256, and HMAC hashing. RSA 2048 roughly equates to AES-112, though AES has no known algorithm weaknesses.
- TPM 2.0 chips interface with UEFI and Windows Boot Loader to check system integrity before releasing any keys.
- TPM 2.0 chips have more software support, especially from Microsoft, allowing them to be used to store passwords and perform automatic authentication for applications such as Outlook.

Operating System Strengths and Weaknesses

Windows: Security over Flexibility

Pros:	Cons:
• TPM support built into the Windows Boot Loader allows boot partition encryption. • User-friendly GUI set-up using Bitlocker.	• Windows installations are hardware-specific and any processor architecture change or core count change will require an operating system re-install. • Configuring the TPM requires partitions to be re-encrypted.

Linux: Flexibility over Security

Pros:	Cons:
• Linux provides the flexibility of being able to swap processors of various architectures. • Linux does not require partitions to be re-encrypted should the operating system change.	• GRUB Boot Loader does not yet have TPM support to handle partition decryption before the operating system is loaded. This means your operating system partition cannot be encrypted.

Migration with Windows Operating Systems

Compatible Windows Versions

Not all Windows versions support BitLocker. Those that do support both TPM 1.2 and TPM 2.0 chips. Versions of Windows prior to Windows 7 do not have TPM/BitLocker support.

Table 1: Compatible Versions of Windows

Versions	Editions
Windows 7	Enterprise or Ultimate
Windows 8	Professional or Enterprise
Windows 10	Professional, Enterprise, or Education

Windows Software Implementation

Windows BitLocker can differentiate between both TPM 1.2 and TPM 2.0. As such there is no difference to the user-end of the software or the installation process.

Migration between TPM 1.2 and 2.0 with Windows

1. With power removed, swap your old TPM 1.2 Bay Trail CPU module with your new TPM 2.0 Bay Trail CPU module.
2. Add power and boot your system.
3. Provide Windows Boot Loader with the recovery key for your boot partition.
4. Unlock all encrypted partitions, including boot, with their respective recovery keys using Bit Locker.
5. Re-encrypt each partition with a newly generated key, write down or save your recovery keys to a USB drive.

Windows installations are built specifically for the processor architecture of the system. Moving a Windows installation to a different system must take this into account by having a compatible processor architecture or doing a full operating system re-install and BitLocker encryption on the boot partition. When upgrading a TPM 1.2 Bay Trail CPU to a TPM 2.0 Bay Trail, the architecture will be compatible so long as the processor core count remains the same, i.e. if you had a quad-core then you must replace it with a quad-core to avoid re-installing Windows.

Migration with Linux Operating Systems

Linux Considerations

Unlike the Windows Boot Loader, TPM software is not built into the Linux GRUB Boot Loader (as of June 2020), making TPM usage less secure and much more difficult to install. In addition, the driver software for TPM 2.0 chips is not officially supported by most Linux distributions. TPM 2.0 drivers can be found on Git Hub, which are open source and development is led by an Intel software engineer. Compared to the TPM 1.2 Linux driver support by most Linux distributions (trousers), the TPM 2.0 drivers from Git Hub are more complicated to use and require many more support libraries. Refer to the RTD "TPM Implementation User's Manual" for instructions on TPM 2.0 software installation. Installation was tested and developed on the 3 most recent Ubuntu LTS; 16.04, 18.04, 20.04.

Migration between TPM 1.2 and 2.0 with Linux

1. Boot your system to an install CD or bootable USB drive containing a Debian-based Linux Distribution installer.
2. During installation partition selection choose the "Do Something Else" option.
3. Select your prior boot partition and set the mount point to " / ". If you followed the TPM 1.2 instructions from the RTD "TPM Implementation User's Manual" this will be the only unencrypted partition. Select "Do Not Use" for all other partitions and make sure the format check box is NOT ticked.
4. The installer may ask you to format the new boot partition, check it is not asking to format any other partitions.
5. Finish installation of the clean Debian-based Linux distribution over your prior boot partition. Do not modify your encrypted partitions.
6. Install TPM 2.0 libraries using process from the RTD "TPM Implementation User's Manual."
7. Set up the TPM 2.0 chip to contain the encryption key for each encrypted partition.
8. Reboot your system to check that all encrypted partitions were unlocked automatically.

Most Linux distributions will tolerate a processor architecture change without an operating system reinstall, however some system stability issues may occur. If both processors have the same version of TPM chip, then it is possible to have the key in both devices' TPM chips to facilitate processor or drive swaps without losing access to encrypted files. Since Linux cannot encrypt the boot partition, you can easily re-install your operating system on the boot partition without losing the files on the encrypted partition. This allows for the processor swap to also change TPM versions from both 1.2 to 2.0 and 2.0 to 1.2 so long as they use compatible keys.

Sales Support

For sales inquiries, you can contact RTD Sales via the following methods:

Phone:	1-814-234-8087, Monday through Friday, 8:00 am to 5:00 pm (ET).
Email:	sales@rtd.com

Technical Support

For help with this product, or any other product made by RTD, you can contact RTD technical support via the following methods:

Phone:	1-814-234-8087, Monday through Friday, 8:00 am to 5:00 pm (ET).
Email:	techsupport@rtd.com

References

The following is a list of references used throughout this design.

Title	Description	Source
TPM Summary and Operation	An in-depth white paper on how the TPM works.	https://trustedcomputinggroup.org/resource/trusted-platform-module-tpm-summary/
RTD TPM Implementation User's Manual	An in-depth white paper on RTD hardware and software of the TPM module.	https://www.rtd.com/manuals/tpm/RTD_TPM_manual.pdf