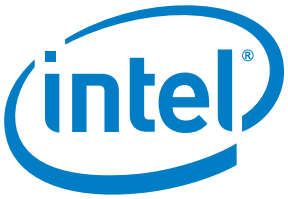

Basic TPM Operations for UTX-3110

Questions? aamir.b.yunus@intel.com

Contents

Figures

§

1 Basic TPM Operations

1.1 Introduction

This guide for UTX-3110 will help you with basic TPM operations such as how to enable TPM, take ownership, clear TPM, create keys. This is by no means a comprehensive guide. It has just enough to get you started.

1.1.1 Enabling TPM in the BIOS

Enabling TPM option in BIOS can be found under Advanced→Trusted Computing menu. See Figure 1 It might be **Disabled** for you.

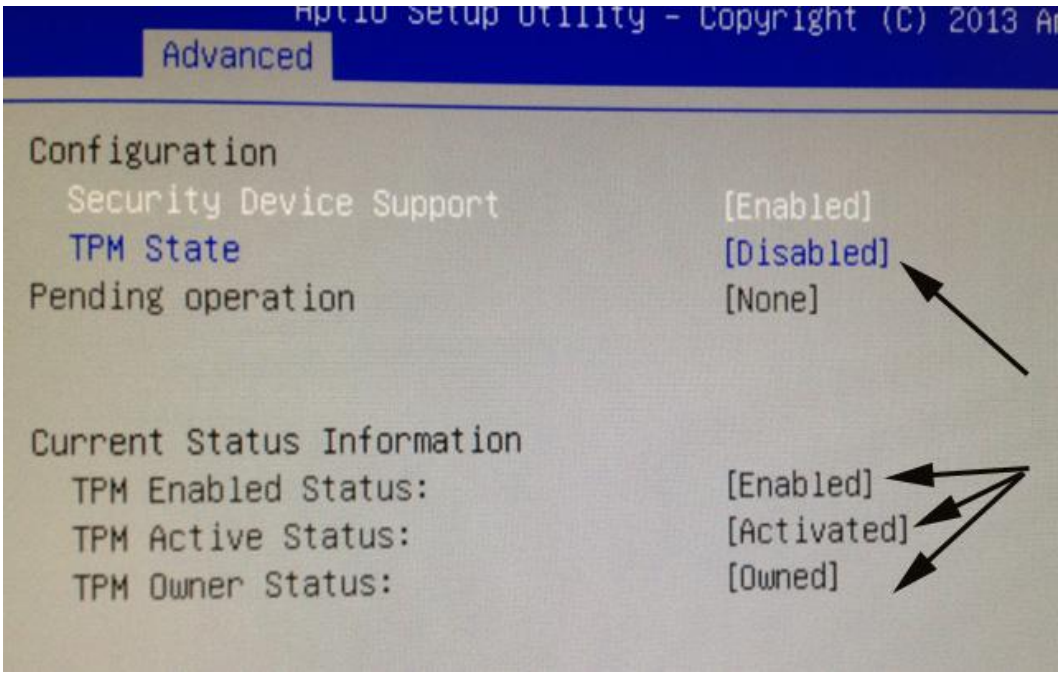

Figure 1. TPM enabling in BIOS

Change the TPM state to **Enabled** as shown in Figure 2. Reboot your Gateway.

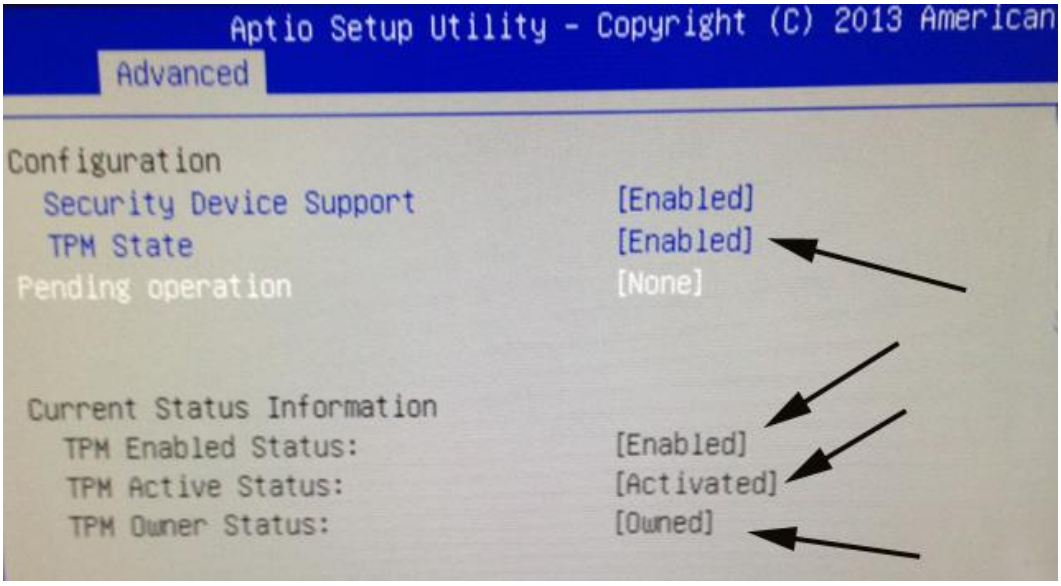

Figure 2. Change TPM State to Enabled

Reboot in BIOS and go to the **Trusting Computing** menu and use arrow keys to go to Pending Operation. That will bring up a pop-up menu as shown in Figure 3. Select **Enable Take Ownership**. **Save, Exit** and reboot your gateway. It might take 2-3 minutes on Verified Booting screen before you get the login prompt.

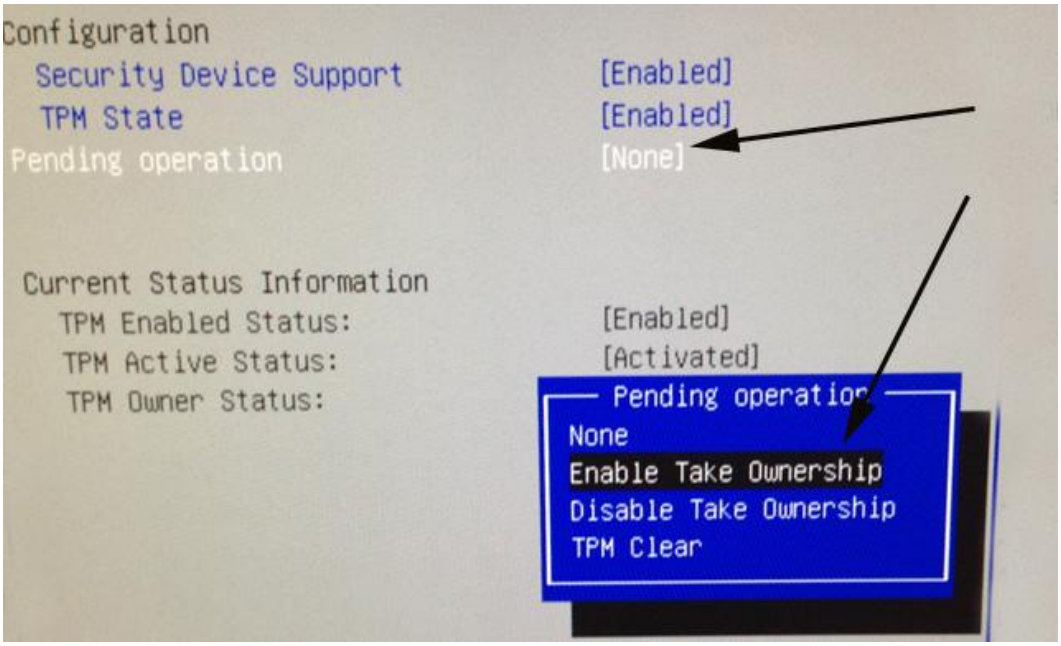

Figure 3. Select Pending Operation

Run the command `tpm_statistic` as shown in Figure 4. You will see that TPM is not cleared.

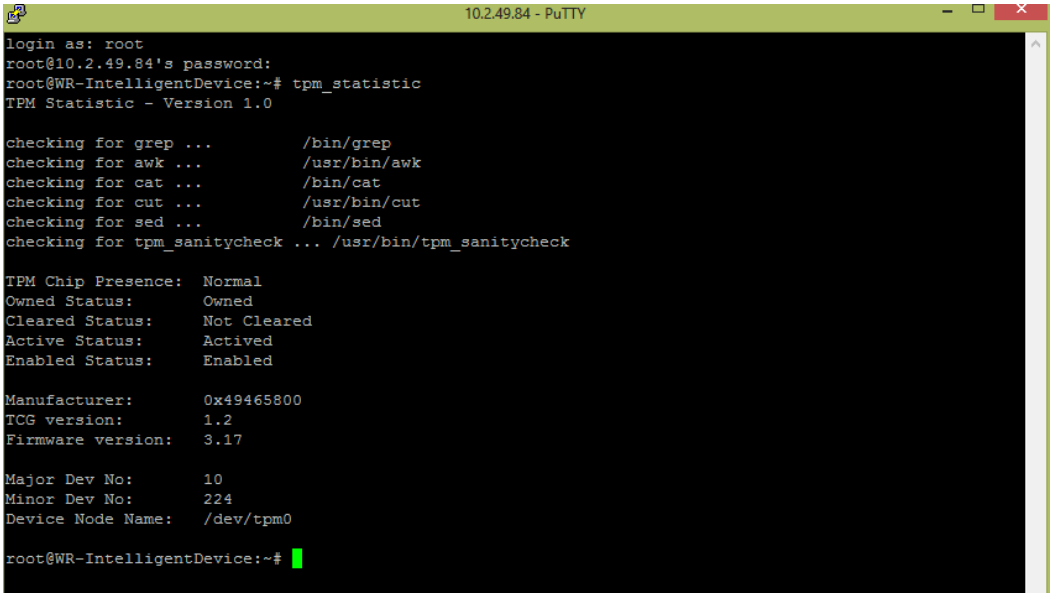

Figure 4. tpm_statistic

Try to clear the TPM by running tpm_clear as shown in Figure 5 Since you have not set the password, you will get an authentication error.

1.1.2 Clearing TPM

Figure 5. tpm_clear

Run the command shown in Figure 6 and enter your password for SRK and owner. For testing, I have used 1234567890 for both.

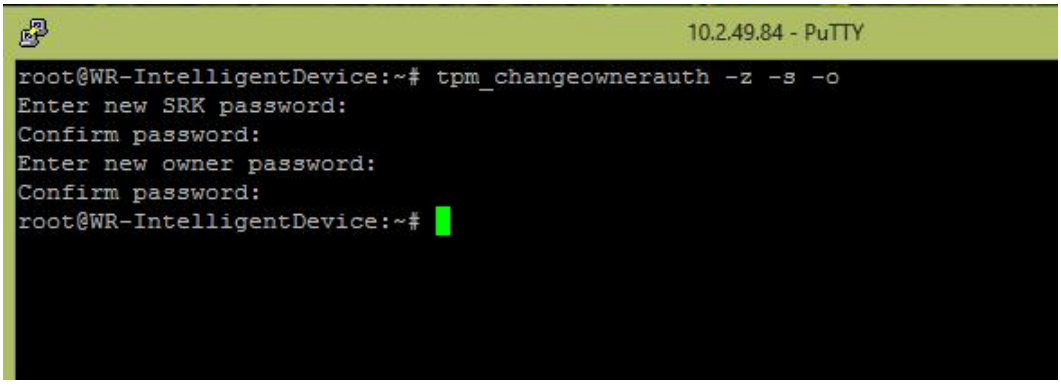

Figure 6. tpm_changeownerauth

Now you can run tpm_clear. You will get a message that TPM is successfully cleared as shown in Figure 7. You will have to enable TPM again in BIOS. If you run tpm_statistic now, you will see that it is cleared as shown in Figure 8

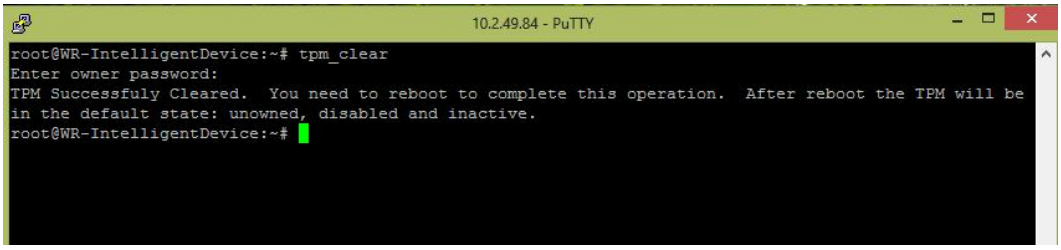

Figure 7. TPM successfully cleared

```
root@WR-IntelligentDevice:~# tpm_statistic
TPM Statistic - Version 1.0

checking for grep ...          /bin/grep
checking for awk ...           /usr/bin/awk
checking for cat ...           /bin/cat
checking for cut ...           /usr/bin/cut
checking for sed ...           /bin/sed
checking for tpm_sanitycheck ... /usr/bin/tpm_sanitycheck

TPM Chip Presence:  Normal
Owned Status:       Not Owned
Cleared Status:     Cleared
Active Status:      Not Actived
Enabled Status:     Disabled

Manufacturer:       0x49465800
TCG version:        1.2
Firmware version:   3.17

Major Dev No:       10
Minor Dev No:       224
Device Node Name:   /dev/tpm0

root@WR-IntelligentDevice:~#
```

Figure 8. tpm_statistic showing it is cleared

1.1.3 Creating Keys

Before creating keys, if your TPM is clear, set the passwords as shown in Figure 9 below.

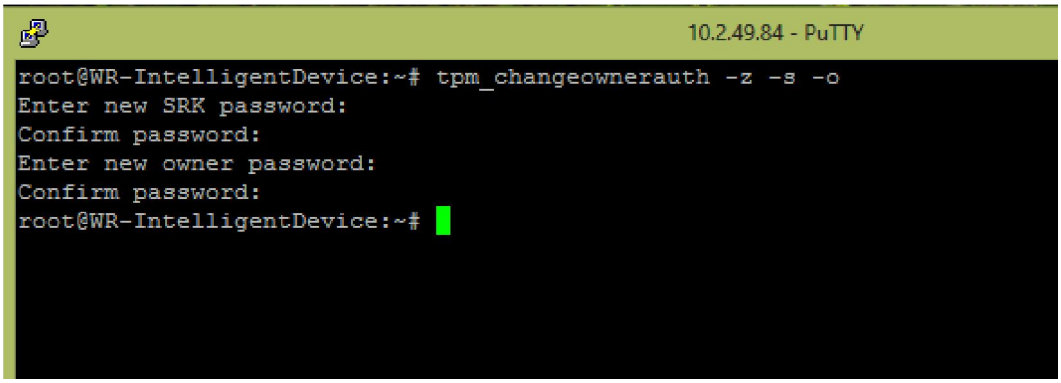

Figure 9. tpm_changeownerauth

You can run `create_tpm_key` command to create key. Your `rootkey.pem` will be created in your working directory. See Figure 10 below. `create_tpm_key --help` gives description of different options available.

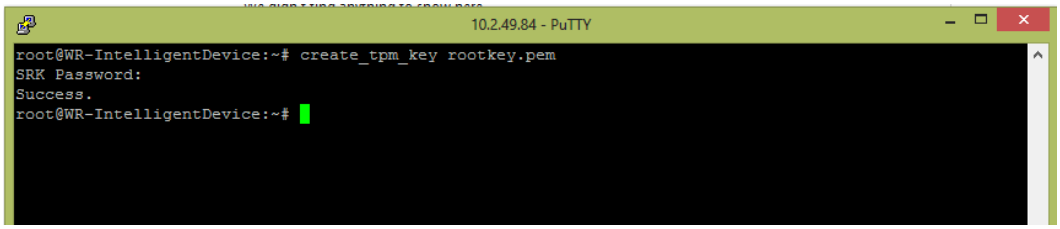

Figure 10. create key

You can also wrap a software key into TPM. Wrapping means encryption which stores the base-64 PEM-formatted software key into the TPM, wraps it with the SRK key, and creates the output index file `rootkey.pem`.

Create a key using OpenSSL. See Figure 11below:

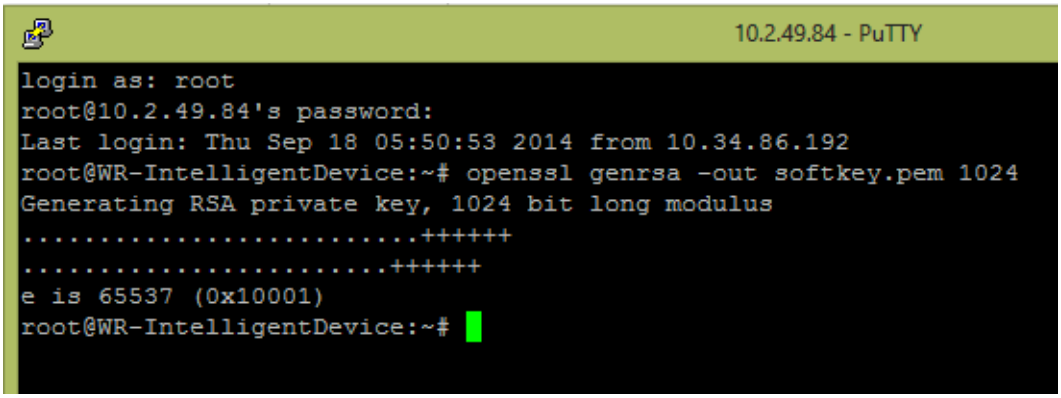

Figure 11. Generate 1024-bit RSA key using OpenSSL

Now you can wrap it by following command shown in Figure 12 below.

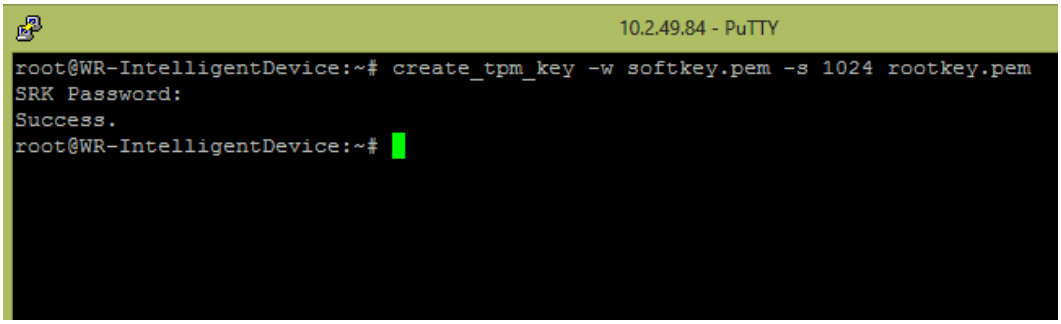

Figure 12. Key wrapping into TPM

1.1.4 TPM Commands

Type tpm_ and then TAB key. It will show you available TPM commands for your Gateway.