ADVANTECH
Enabling an Intelligent Planet

Advantech AE Technical Share Document

Date	05 / 05 / 2022	**Release Note**	□ Internal ■ External
Category	■ FAQ □ SOP	**Related OS**	Linux
Abstract	How to initialize and simply test TPM in Linux		
Keyword	Linux, TPM		
Related Product	All platforms with TPM installed		

- **Conditions:**

  Platform: UNO-420 (Intel Bay Trail)
  OS: Ubuntu desktop 18.04.6
  TPM: Infineon SLB9665TT2.0 FW5.62

- **Brief Solution - Step by Step:**

  In Ubuntu 18.04.6, it requires installing the following package for initializing TPM.
  In Ubuntu 20.04, it has included all the related TPM packages, please directly jump to **Clear TPM**.

For Ubuntu Ubuntu 18.04

First, you can install all the dependencies in one go:

```
#sudo apt -y install \
   autoconf-archive \
   libcmocka0 \
   libcmocka-dev \
   build-essential \
   git \
   pkg-config \
   gcc \
   g++ \
   m4 \
   libtool \
   automake \
   autoconf \
   libdbus-glib-1-dev \
   libssl-dev \
   glib2.0 \
   cmake \
   libssl-dev \
   libcurl4-gnutls-dev
   libjson-c-dev
```

Install tpm2-tss

Once you are done with that, you need to build and install the TPM Software Stack (tpm2-tss) library

Download & Build:

```
#git clone https://github.com/tpm2-software/tpm2-tss.git
#cd tpm2-tss
# ./bootstrap
#./configure --with-udevrulesdir=/etc/udev/rules.d
#make
#sudo make install
#sudo ldconfig
#cd ..
```

Install tpm2-abrmd

The next tool we need is the TPM Access Broker and Resource Manager

Adding user:

```
#sudo useradd --system --user-group tss
```

Download & Build:

```
#git clone https://github.com/tpm2-software/tpm2-abrmd.git
#cd tpm2-abrmd
#./bootstrap
#./configure --with-dbuspolicydir=/etc/dbus-1/system.d --with-systemdsystemunitdir=/lib/systemd/system
#make
#sudo make install
#cd ..
```

Post-build:

```
#sudo udevadm control --reload-rules && sudo udevadm trigger
#sudo pkill -HUP dbus-daemon
```

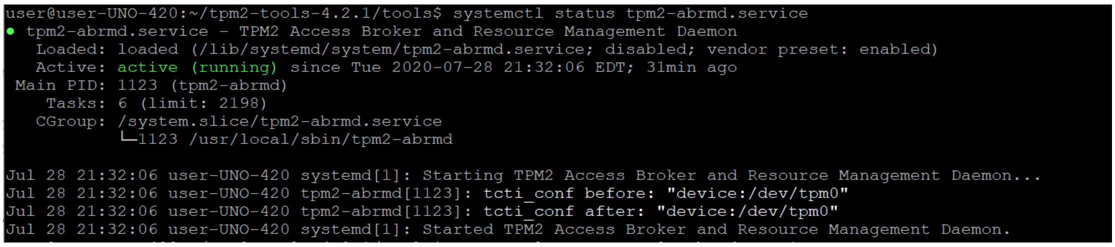
```
#sudo systemctl daemon-reload
#sudo ldconfig
#sudo systemctl enable tpm2-abrmd
#sudo service tpm2-abrmd start
```

You can verify that this was installed successfully by checking the status:

```
#systemctl status tpm2-abrmd.service
```

Which should give you an output like the following:

● tpm2-abrmd.service - TPM2 Access Broker and Resource Management Daemon



```
user@user-UNO-420:~/tpm2-tools-4.2.1/tools$ systemctl status tpm2-abrmd.service
● tpm2-abrmd.service - TPM2 Access Broker and Resource Management Daemon
   Loaded: loaded (/lib/systemd/system/tpm2-abrmd.service; disabled; vendor preset: enabled)
   Active: active (running) since Tue 2020-07-28 21:32:06 EDT; 31min ago
 Main PID: 1123 (tpm2-abrmd)
    Tasks: 6 (limit: 2198)
   CGroup: /system.slice/tpm2-abrmd.service
           └─1123 /usr/local/sbin/tpm2-abrmd

Jul 28 21:32:06 user-UNO-420 systemd[1]: Starting TPM2 Access Broker and Resource Management Daemon...
Jul 28 21:32:06 user-UNO-420 tpm2-abrmd[1123]: tcti_conf before: "device:/dev/tpm0"
Jul 28 21:32:06 user-UNO-420 tpm2-abrmd[1123]: tcti_conf after: "device:/dev/tpm0"
Jul 28 21:32:06 user-UNO-420 systemd[1]: Started TPM2 Access Broker and Resource Management Daemon.
```

Install tpm2-tools

Download TPM2-Tools:

```
#sudo apt-get install tpm2-tools
```

OR build by yourself as the following steps:

The third tool to install is the TPM 2 Tools

Download & Build:

```
#git clone https://github.com/tpm2-software/tpm2-tools.git
#./bootstrap
#./configure
#make
#sudo make install
#cd ..
```

```
#export TPM2TOOLS_DEVICE_FILE="/dev/tpmrm0"
#export TPM2TOOLS_TCTI_NAME="device"
```

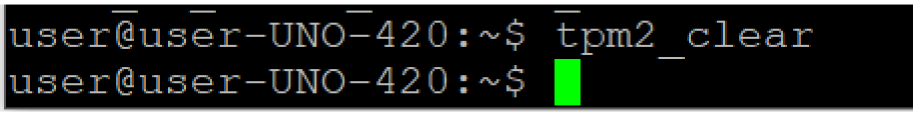
Need to disable trousers service:

```
#systemctl stop trousers.service
```

```
#systemctl disable trousers.service
```

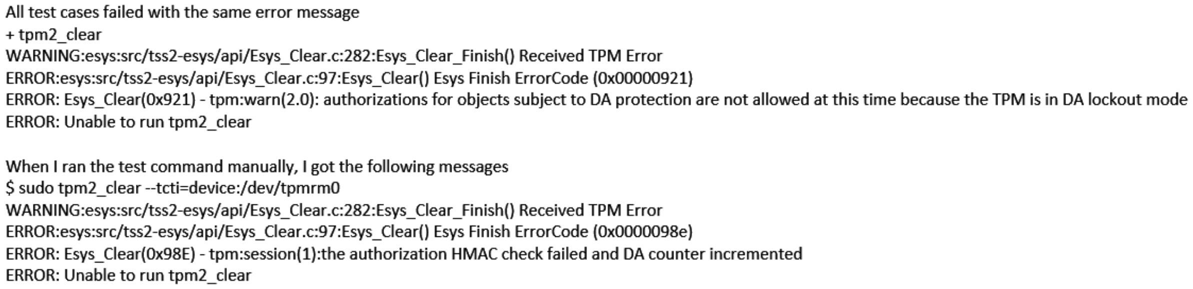
Clear TPM

If your TPM has been used before, it requires to clear TPM before using again.
After booting and into the Ubuntu, you can run following command to clear TPM.



```
user@user-UNO-420:~$ tpm2_clear
user@user-UNO-420:~$
```

If you have the same error as below when running tpm2_clear, the error indicates that TPM is in DA lockout mode



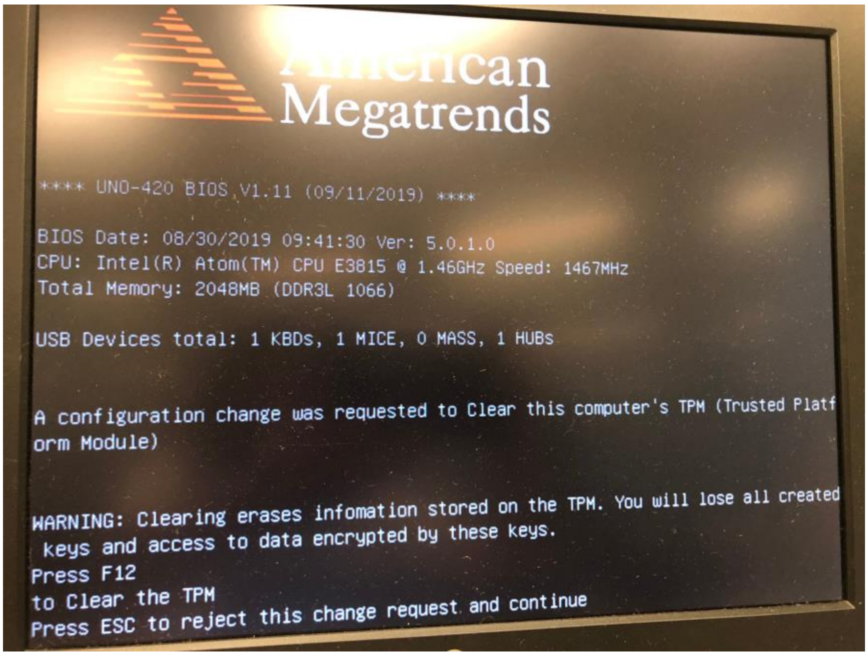
```
All test cases failed with the same error message
+ tpm2_clear
WARNING:esys:src/tss2-esys/api/Esys_Clear.c:282:Esys_Clear_Finish() Received TPM Error
ERROR:esys:src/tss2-esys/api/Esys_Clear.c:97:Esys_Clear() Esys Finish ErrorCode (0x00000921)
ERROR: Esys_Clear(0x921) - tpm:warn(2.0): authorizations for objects subject to DA protection are not allowed at this time because the TPM is in DA lockout mode
ERROR: Unable to run tpm2_clear

When I ran the test command manually, I got the following messages
$ sudo tpm2_clear --tcti=device:/dev/tpmrm0
WARNING:esys:src/tss2-esys/api/Esys_Clear.c:282:Esys_Clear_Finish() Received TPM Error
ERROR:esys:src/tss2-esys/api/Esys_Clear.c:97:Esys_Clear() Esys Finish ErrorCode (0x0000098e)
ERROR: Esys_Clear(0x98E) - tpm:session(1):the authorization HMAC check failed and DA counter incremented
ERROR: Unable to run tpm2_clear
```

Please restart the system and enter the BIOS to clear TPM.
BIOS->Advanced->Trustd computing->Pending Operation->TPM clear

If your BIOS does not have the above option, you can follow the below steps to clear TPM.
In order to trigger a clear apparently this is the way:

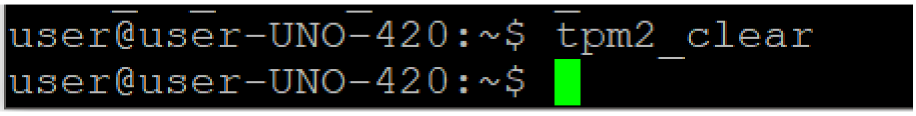
```
#echo 5 > /sys/class/tpm/tpm0/ppi/request
#reboot
```

The BIOS/UEFI then asks for confirmation to reset the TPM. While booting, you will see the following screen, then press F12 to clear erase information in TPM.



```
**** UNO-420 BIOS V1.11 (09/11/2019) ****

BIOS Date: 08/30/2019 09:41:30 Ver: 5.0.1.0
CPU: Intel(R) Atom(TM) CPU E3815 @ 1.46GHz Speed: 1467MHz
Total Memory: 2048MB (DDR3L 1066)

USB Devices total: 1 KBDs, 1 MICE, 0 MASS, 1 HUBs


A configuration change was requested to Clear this computer's TPM (Trusted Platf
orm Module)


WARNING: Clearing erases infomation stored on the TPM. You will lose all created
 keys and access to data encrypted by these keys.
Press F12
to Clear the TPM
Press ESC to reject this change request and continue
```

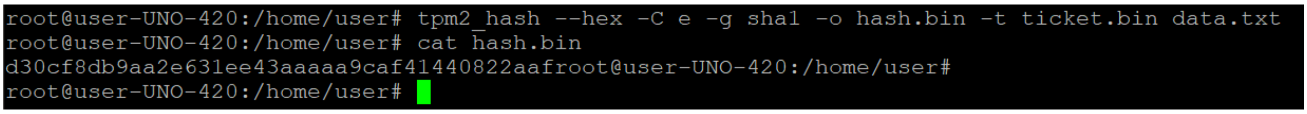
After booting and into the Ubuntu, you can run the tpm2_clear command again, there should be no error.



```
user@user-UNO-420:~$ tpm2_clear
user@user-UNO-420:~$ 
```

Hash by TPM

#echo “my message” > data.txt
#tpm2_hash -C e -g sha1 -o hash.bin -t ticket.bin data.txt



```
root@user-UNO-420:/home/user# tpm2_hash --hex -C e -g sha1 -o hash.bin -t ticket.bin data.txt
root@user-UNO-420:/home/user# cat hash.bin
d30cf8db9aa2e631ee43aaaaa9caf41440822aafroot@user-UNO-420:/home/user#
root@user-UNO-420:/home/user# 
```

You can get more information by tpm2_hash --help

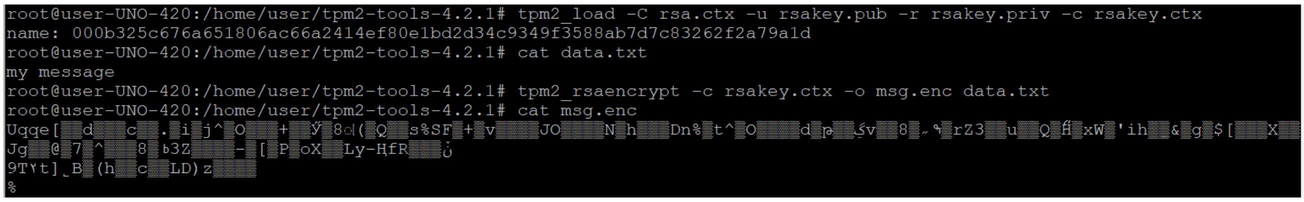
RSA encrypt the file

Create an RSA key and load it

#tpm2_createprimary -c rsa.ctx
#tpm2_create -C rsa.ctx -Grsa2048 -u rsakey.pub -r rsakey.priv
#tpm2_load -C rsa.ctx -u rsakey.pub -r rsakey.priv -c rsakey.ctx

Encrypt using RSA

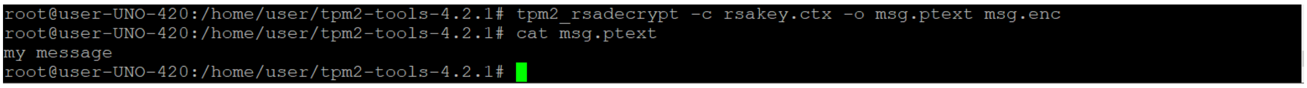
#echo “my message” > data.txt
#tpm2_rsaencrypt -c rsakey.ctx -o msg.enc data.txt



```
root@user-UNO-420:/home/user/tpm2-tools-4.2.1# tpm2_load -C rsa.ctx -u rsakey.pub -r rsakey.priv -c rsakey.ctx
name: 000b325c676a651806ac66a2414ef80e1bd2d34c9349f3588ab7d7c83262f2a79a1d
root@user-UNO-420:/home/user/tpm2-tools-4.2.1# cat data.txt
my message
root@user-UNO-420:/home/user/tpm2-tools-4.2.1# tpm2_rsaencrypt -c rsakey.ctx -o msg.enc data.txt
root@user-UNO-420:/home/user/tpm2-tools-4.2.1# cat msg.enc
Uqqe[▒▒d▒▒▒c▒▒.▒i▒j^▒O▒▒▒+▒▒Ý▒8(▒Q▒▒s%SF▒+▒v▒▒▒▒JO▒▒▒▒N▒h▒▒▒Dn%▒t^▒O▒▒▒▒d▒p▒▒ś v▒▒8▒.▒rZ3▒▒u▒▒Q▒Ĥ▒xW▒'ih▒▒&▒g▒$[▒▒▒X▒▒
Jg▒▒@▒7▒^▒▒▒8▒b3Z▒▒▒▒-▒[▒P▒oX▒▒Ly-ĦfR▒▒▒ỏ
9T۲t]_B▒(h▒▒c▒▒LD)z▒▒▒▒
%
```

Decrypt using RSA

#tpm2_rsadecrypt -c rsakey.ctx -o msg.ptext msg.enc



```
root@user-UNO-420:/home/user/tpm2-tools-4.2.1# tpm2_rsadecrypt -c rsakey.ctx -o msg.ptext msg.enc
root@user-UNO-420:/home/user/tpm2-tools-4.2.1# cat msg.ptext
my message
root@user-UNO-420:/home/user/tpm2-tools-4.2.1# 
```