The following procedure is not tested to work if there are other products using the TPM. Please consult with your IT staff to ensure nothing else is using the TPM before proceeding.

Required Software:

tpm\_tools.zip

TPM-120106.iso

Step 1:

Boot into BIOS and turn on/activate the TPM. You may have to reboot after turning on the TPM, go back into BIOS and then activate because sometimes the BIOS won’t let you do both at once. If the TPM is already turned on/activated, then clear the TPM via the BIOS.

Step 2:

Note: This step is only required for Dell Latitude laptops that have never been previously provisioned.

Boot off of the “TPM provisioning cd” iso image that is referenced above. Login as “root” and a script will automatically start. Press return at every prompt, accepting the default options, even when it means there is no input (e.g. no hostname). When prompted “Enter owner password”, hit ctrl-c to exit the script, as the necessary key has already been created.

Reboot and return to the BIOS. Select the Clear option for the TPM to clear any TPM credentials the provisioning cd created. The key that was burned onto the TPM chip will remain, even during a TPM clear through the BIOS. If necessary, re-select that you want the TPM to be activated after the clear.

Step 3:

Boot into the host operating system. Extract the tpm\_tools.zip archive so that the tpm\_tools files are located within C:\tpm\_tools. For instance, the file C:\tpm\_tools\createkey.exe should exist and have that exact path. *Right click on cmd.exe and select Run as Administrator*, and then cd into the tpm\_tools directory.

1. Install the opentpm driver by running install\_opentpm.bat
2. Provision the TPM by running provision\_tpm.bat. This will take a long time, so don’t kill the process if it is taking a while.
3. Load the TPM keys by running loadkeys.bat
4. Next we will configure the loadkeys.bat file to run at system startup. Go to start->run and type “gpedit.msc” and hit enter. Expand Computer Configuration->Windows Settings->Scripts. Double click on “startup.” Click “add” then browse to C:\tpm\_tools\loadkeys.bat. Select “loadkeys.bat” and hit ok.
5. Next we will need to place the public portion of the key files created in step 3.C on the Checkmate server so that signatures can be verified during measurements. In the C:\tpm\_tools directory you will find the files “identity.pem” and “signingkey.pem.” Rename these files hostname-identitykey.pem and hostname-signingkey.pem. For instance, if I was provisioning foo.bla.com, I would name the files foo.bla.com-signingkey.pem and foo.bla.com-identitykey.pem. If there is no hostname, then you can name them just –signingkey.pem and –identitykey.pem, but obviously you cannot measure more than one host without a hostname. Next you will need to transfer these two .pem files to server\_trunk\_cut\_release\client\_keys on the Checkmate server.

Step 4:

Reboot and you should now be configured to use both the “PCRS Measurement” and “Tickstamp Attestation” measurement on the server.