Infineon TPM Firmware Update Tools

For use with Linux operating systems

Infineon TPM Factory Update Tool

User's Manual

About this Document

Scope and purpose

This document describes the conditions and usage of Infineon TPM Factory Update Tool in order to update the firmware of an Infineon TPM (Trusted Platform Module).

Intended audience

This document is intended for Infineon TPM customers.

Table of Contents

1 Welcome

Welcome to Infineon TPM Factory Update Tool.

Infineon TPM Factory Update Tool is part of Infineon TPM Firmware Update Tools and is a command line application that enables a manufacturing or service facility to update the firmware of an Infineon TPM (Trusted Platform Module).

This user manual provides information about the preconditions and postconditions (see chapter 3) and about the usage of Infineon TPM Factory Update Tool (see chapter 5).

Note: For latest updates, please refer to Readme.txt provided in the delivery package.

2 Operating Environment

Infineon TPM Factory Update Tool for Linux operating systems is provided as source code under the conditions specified in License.txt.

Chapter 4 shows the preconditions and how to build the Infineon TPM Factory Update Tool.

The source code package can be used on Linux 32-bit and 64-bit operating systems on x86 and ARM platforms. For a list of tested distributions please refer to the Readme.txt.

3 TPM Firmware Update Overview

Since Infineon TPM Factory Update Tool supports updating the firmware of both a TPM1.2 and a TPM2.0 to any of the two TPM families (TPM1.2 or TPM2.0), different preconditions and update scenarios do exist. They will be described in chapter 3.1 and 3.2.

Attention: ***The total number of firmware updates allowed by the TPM is limited (please consult your local Infineon representative for further details). Once the limit has been reached, no further TPM Firmware Update will be possible. It is recommended to first check possibility of further firmware updates using TPMFactoryUpd -info parameter before attempting actual firmware update.***

Attention: ***After performing TPM Firmware Update some postconditions must be fulfilled in order to get the TPM back into a fully functional state. These conditions are listed in chapter 3.4.***

3.1 TPM2.0 Firmware Update

This chapter describes preconditions and scenarios for updating the firmware of a TPM2.0.

3.1.1 Introduction

TPM2.0 Firmware Update authorization is tied to a policy called platformPolicy. Thus, knowing and satisfying platformPolicy is required to start TPM2.0 Firmware Update. The Platform Policy is one of the features of Platform Hierarchy, a TPM2.0 set of features intended for exclusive use by the platform (for example the System Firmware / BIOS). The Infineon TPM Factory Update Tool authorizes a TPM 2.0 Firmware Update by setting the Platform Policy which needs an Empty Buffer platformAuth (see 3.1.2). The following Figure 1 describes the actions the Infineon TPM Factory Update Tool performs to update the TPM 2.0 Firmware.

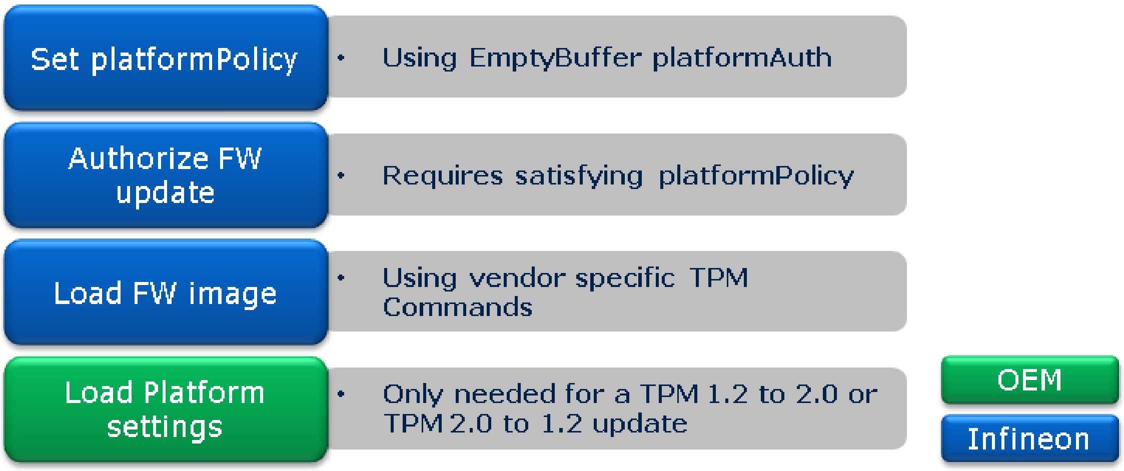
Set platformPolicy
• Using EmptyBuffer platformAuth
Authorize FW update
• Requires satisfying platformPolicy
Load FW image
• Using vendor specific TPM Commands
Load Platform settings
• Only needed for a TPM 1.2 to 2.0 or TPM 2.0 to 1.2 update
OEM
Infineon

Figure 1 High Level Actions

Further, TPM Firmware Update authorization consists of starting an authorized Policy Session and initiate the TPM Firmware Update sequence with that Policy Session. To create the Policy Session the Infineon TPM Factory Update Tool initializes the Platform Policy in the following manner:

platformPolicy = TPM2_PolicySecret(TPM_RH_PLATFORM, ...) AND TPM2_PolicyCommandCode(TPM_CC_FieldUpgradeStartVendor)

Now a Policy Session must be started and updated to satisfy the configured Platform Policy and the session can be used to authorize and start the TPM 2.0 Firmware Update sequence.

Chapter 3.1.3 gives information about the different update scenarios.

3.1.2 Preconditions

Updating the firmware of an Infineon TPM2.0 requires Platform Policy Authorization. To update a TPM2.0 firmware using Infineon TPM Factory Update Tool, the following preconditions must be met:

- Platform hierarchy is enabled
- platformAuth is set to Empty Buffer

Attention: ***platformAuth may be set to EmptyBuffer only when the system is in a controlled manufacturing or service environment. Leaving platformAuth set to EmptyBuffer outside of such an environment may create a security risk.***

3.1.3 Update Scenarios

The scenario for TPM2.0 to TPM1.2 firmware update is shown in Figure 2 and for TPM2.0 to TPM2.0 firmware update in Figure 3.

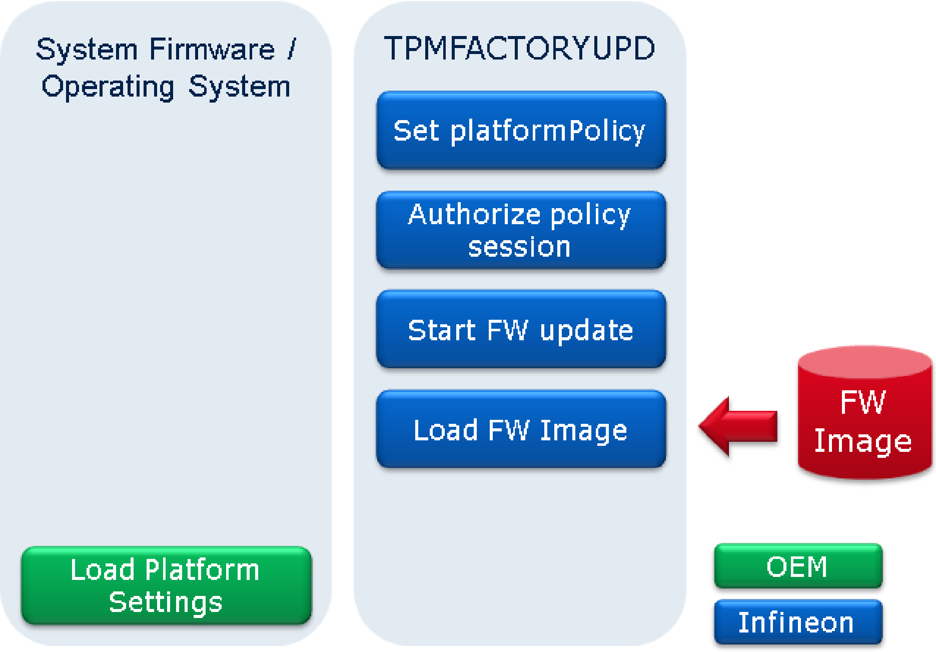

Figure 2 TPM2.0 to TPM1.2 Firmware Update

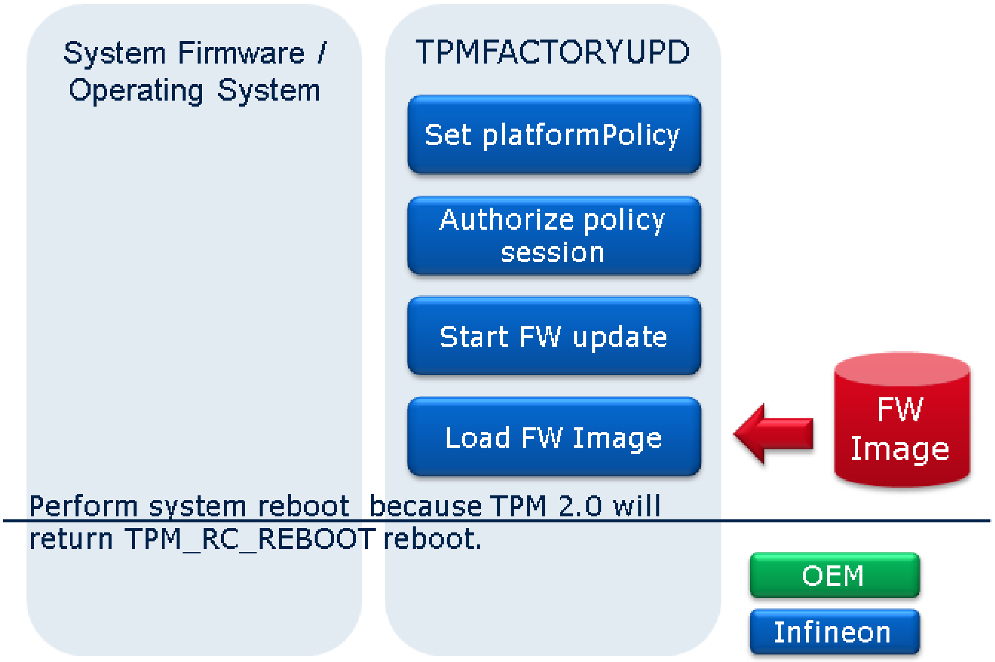
System Firmware / Operating System
TPMFACTORYUPD
Set platformPolicy
Authorize policy session
Start FW update
Load FW Image
FW Image
Perform system reboot because TPM 2.0 will return TPM_RC_REBOOT reboot.
OEM
Infineon

Figure 3 TPM2.0 to TPM2.0 Firmware Update

3.2 TPM1.2 Firmware Update

This chapter describes preconditions and scenarios for updating the firmware of a TPM1.2.

3.2.1 Preconditions

To update a TPM1.2 firmware, two possibilities for authorizing firmware update do exist:

3.2.1.1 Deferred Physical Presence (DPP) authorization

In order to be able to perform a TPM1.2 firmware update using Infineon TPM Factory Update Tool with DPP authorization, the following preconditions must be met:

- Physical Presence (PP) command is available and PP is not locked (required to be able to set DPP) or DPP bit has already been set in the current TPM power cycle
- TPM Ownership has not been taken

Attention: ***The system needs to be in a controlled manufacturing or service environment when the Physical Presence command is not locked. Not locking the Physical Presence command outside such an environment may create a security risk.***

3.2.1.2 TPM Owner authorization

In order to be able to perform a TPM1.2 firmware update using Infineon TPM Factory Update Tool with TPM Owner authorization, the following preconditions must be met:

- TPM is in state enabled and activated
- TPM Ownership has not been taken (since it will be taken by Infineon TPM Factory Update Tool)

3.2.2 Update Scenarios

This chapter describes the update scenarios using different authorization values.

3.2.2.1 Using Deferred Physical Presence Authorization

The scenario using DPP authorization for TPM1.2 to TPM2.0 firmware update is shown in Figure 4 and for TPM1.2 to TPM1.2 firmware update in Figure 5.

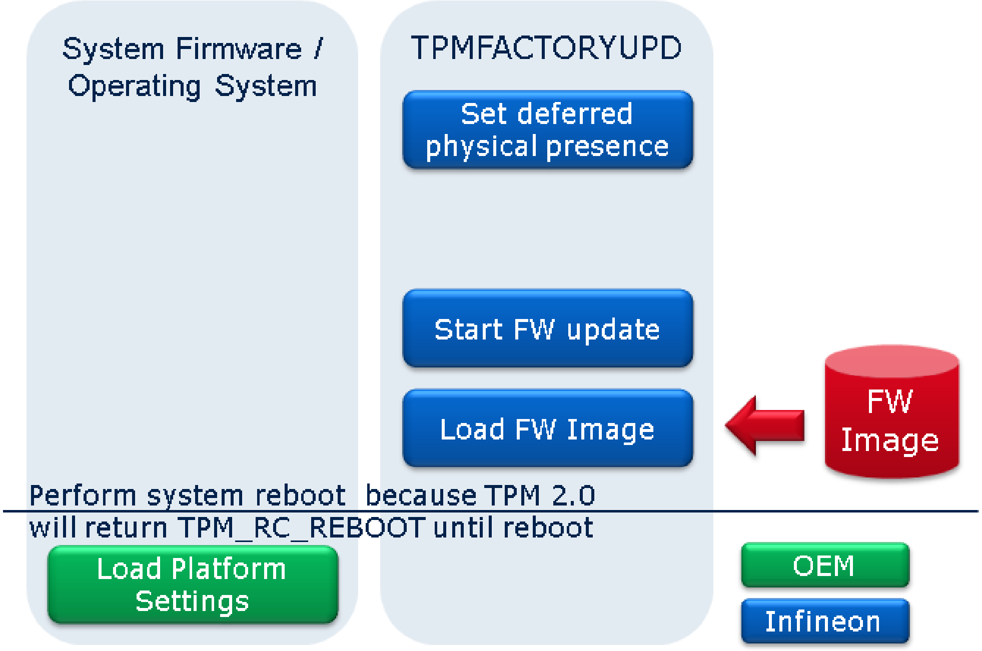
System Firmware / Operating System
TPMFACTORYUPD
Set deferred physical presence
Start FW update
Load FW Image
FW Image
Perform system reboot because TPM 2.0 will return TPM_RC_REBOOT until reboot
Load Platform Settings
OEM
Infineon

Figure 4 TPM1.2 to TPM2.0 Firmware Update using Deferred Physical Presence authorization

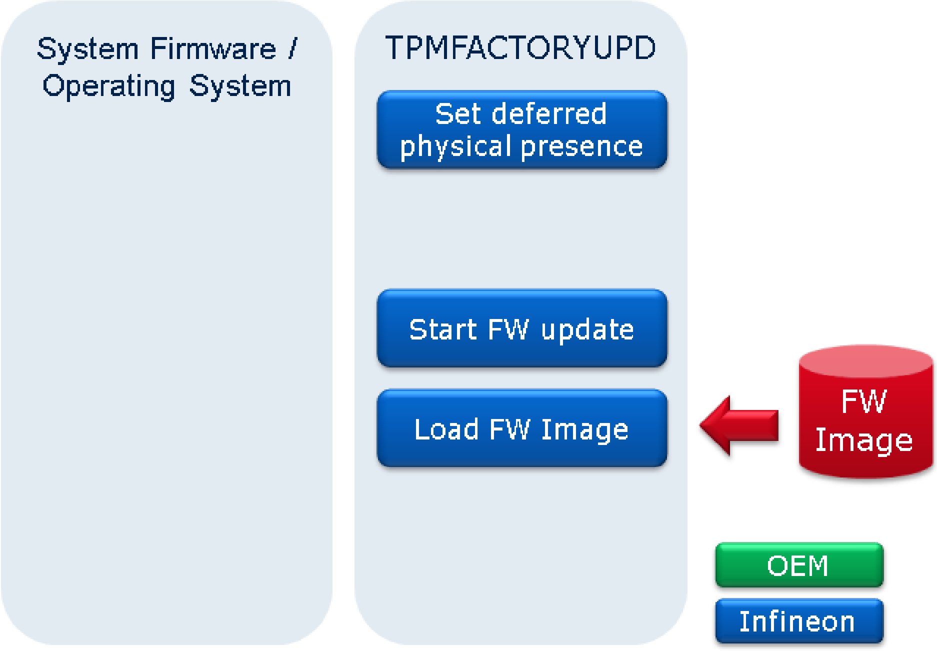
System Firmware / Operating System
TPMFACTORYUPD
Set deferred physical presence
Start FW update
Load FW Image
FW Image
OEM
Infineon

Figure 5 TPM1.2 to TPM1.2 Firmware Update using Deferred Physical Presence authorization

3.2.2.2 Using TPM Owner Authorization

The scenario using TPM Owner authorization for TPM1.2 to TPM2.0 firmware update is shown in Figure 6 and for TPM1.2 to TPM1.2 firmware update in Figure 7.

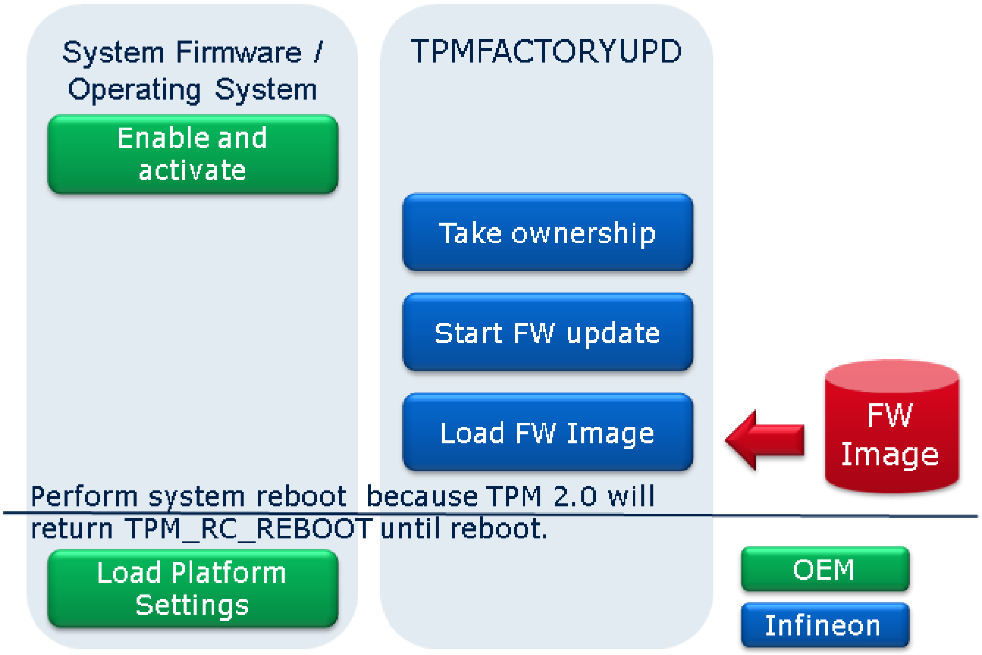

Figure 6 TPM1.2 to TPM2.0 Firmware Update using TPM Owner authorization

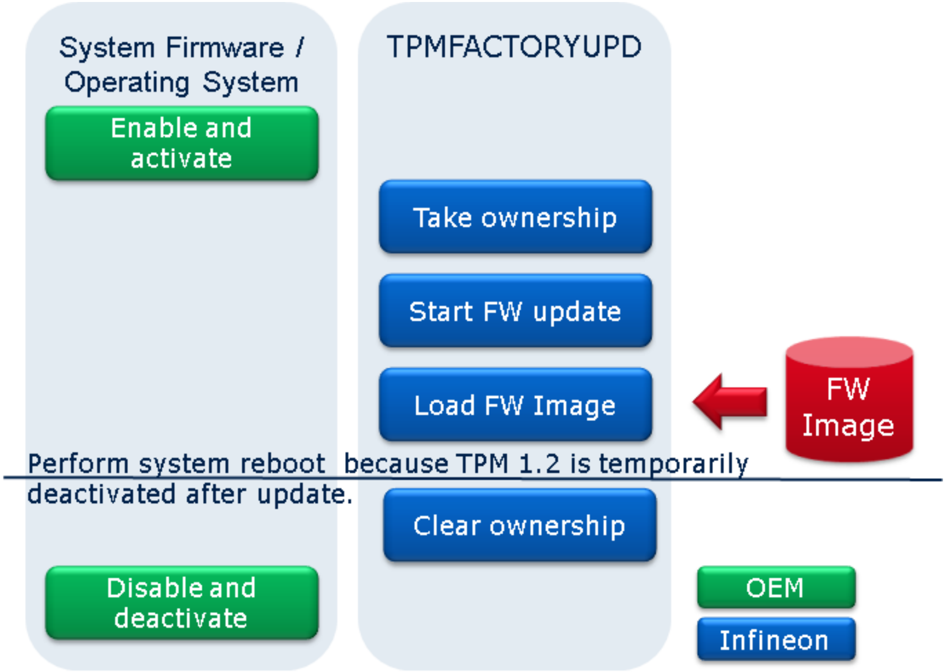

Figure 7 TPM1.2 to TPM1.2 Firmware Update using TPM Owner authorization

3.3 Cross Version Update

For the cross version update path, the TPM will be reset to factory defaults (also referred to as Manufacturing Mode) after a successful update. All data and state from the old TPM firmware will be lost (for example: keys used for drive or data encryption, NV indices, TxT related data, etc.). The System Firmware or other tools must reload the Platform Settings into the TPM after TPM Firmware Update is complete. The Infineon TPM Factory Update Tool shows the information about the reset to factory defaults during the update (see chapter 5.4.1).

3.3.1 Update a TPM2.0 to TPM1.2

If Infineon TPM Factory Update Tool changes a TPM2.0 to a TPM1.2:

- The System Firmware should configure physicalPresenceHWEnable and physicalPresenceCMDEnable and set physicalPresenceLifetimeLock.
- The System Firmware should configure NV Storage area (for example: store EK credential or platform credential) and enforce NV authorizations with TPM_NV_DefineSpace(TPM_NV_INDEX_LOCK).
- The System Firmware should initialize delegate tables if required.

For more details refer to the corresponding Basic Platform Manufacturer Guidelines [1], [2] for your TPM Model which can be requested from your local Infineon representative.

3.3.2 Update a TPM1.2 to TPM2.0

If Infineon TPM Factory Update Tool changes a TPM1.2 to a TPM2.0:

- The System Firmware should create Platform Hierarchy keys if required.
- The System Firmware should create NV indices if required.

For more details refer to the TPM2.0 User Guidance [3] which can be requested from your local Infineon representative.

3.4 Postconditions

In case of any TPM Firmware Update with a target firmware belonging to the TPM2.0 family, the TPM is in “Reboot Required” mode after a successful firmware update. This mode remains until the next TPM reset.

In case of any TPM Firmware Update with a target firmware belonging to the TPM1.2 family, the TPM is temporarily deactivated after a successful firmware update. This mode remains until the next TPM reset.

In case of a TPM Firmware Update with TPM Owner authorization with both source and target version belonging to the TPM1.2 family, the TPM has an owner after the update. The owner secret is the SHA-1 hash of the ASCII-encoded string “12345678” (without “” characters). The TPM Ownership can be cleared after the next TPM reset using Infineon TPM Factory Update Tool (see chapter 5.4.4).

Attention: ***It is recommended to always restart the system directly after the TPM Firmware Update, since certain system hardware and software components might not be aware of a TPM Firmware Update without a restart (especially in case the TPM family has been changed with the update.)***

3.5 Resume an Interrupted TPM Firmware Update

In case TPM Firmware Update has been interrupted during any of the described update scenarios, the TPM will support only a limited number of TPM commands, thus it is likely that the TPM device will not be available to the Operating System at all or will be present as a non-functional device. Therefore, it is critical that the TPM firmware recovery is done immediately. The Infineon TPM Factory Update Tool detects the “Invalid Firmware Mode” according to the following flow chart. The System Firmware or other tools can use the same flow chart to detect the “Invalid Firmware Mode”. The TPM behavior after an interrupted Firmware Update is the same whether the TPM Firmware Update was started on a TPM1.2 or TPM2.0.

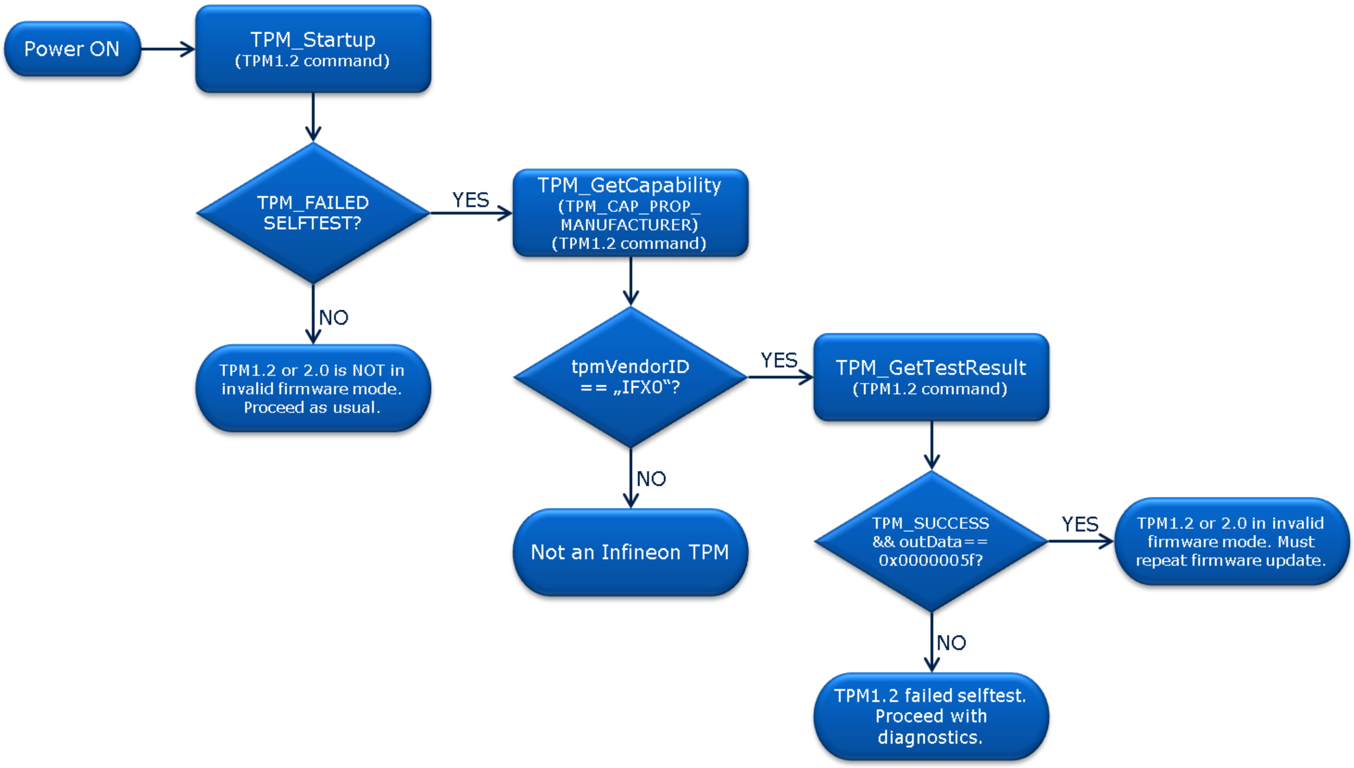
Power ON
TPM_Startup
(TPM1.2 command)
TPM_FAILED SELFTEST?
YES
NO
TPM_GetCapability
(TPM_CAP_PROP_ MANUFACTURER)
(TPM1.2 command)
TPM1.2 or 2.0 is NOT in invalid firmware mode. Proceed as usual.
tpmVendorID == „IFX0"?
YES
NO
TPM_GetTestResult
(TPM1.2 command)
Not an Infineon TPM
TPM_SUCCESS && outData== 0x0000005f?
YES
NO
TPM1.2 or 2.0 in invalid firmware mode. Must repeat firmware update.
TPM1.2 failed selftest. Proceed with diagnostics.

Figure 8 Invalid Firmware Mode Detection

Attention: ***It must be ensured that the TPM Firmware Update is resumed with the same firmware image that has been used when the TPM Firmware Update was interrupted.***

Attention: ***The number of resume attempts is limited. For the exact number of resume attempts supported by a particular TPM model please consult the TPM documentation or contact your local Infineon representative.***

Note: *Make sure to cycle power to the TPM once (for example by shutting down the system) before starting the resume attempt.*

3.6 Naming of Firmware Images

Firmware image files follow a specific naming scheme:

[Source]_[Version]_to_[Target]_[Version].bin

Place holder values:

- Source = { TPM12, TPM20 }
- Target = { TPM12, TPM20}
- Version = version of firmware (for example: 1.23.456.0)

For example a firmware image file could be named TPM12_1.22.333.0_to_TPM20_1.23.456.0.bin. This would mean that the firmware image file would update a TPM1.2 with firmware version 1.22.333.0 to a TPM2.0 with firmware version 1.23.456.0.

Please consult your local Infineon representative for further details of a firmware image file (for example, to which firmware version(s) the update can be applied).

4 Building the Tool

This chapter describes how the Infineon TPM Factory Update Tool can be compiled and which preconditions must be fulfilled.

4.1 Preconditions

The following conditions must be fulfilled:

- Unpack the source code to a full accessible folder on the target system.
- The libssl-dev library must be installed.

For a list of supported and tested Linux distributions please refer to the Readme.txt.

4.2 Compilation

To compile and run the Infineon TPM Factory Update Tool follow the steps below:

- Open a terminal
- Change directory to the unpacked source code
- Change directory to “Source/TPMFactoryUpd”
- Call “make” to compile the Infineon TPM Factory Update Tool.
  Use “make debug” to create a TPMFactoryUpd executable which can be debugged with gdb or other debuggers.
- Call sudo “TPMFactoryUpd –info”. If everything is configured well the tool will show the current state of the TPM. Otherwise an error message is shown and must be analysed. Please refer to chapter 5.1 and 5.5 for more information about the usage and the tools return codes.

5 Using the Tool

Infineon TPM Factory Update Tool is a command line application. Its command line options and return codes are described in detail in the next chapters.

5.1 Command Line Parameters

The following command line parameters shown in Table 1 are supported:

Table 1 Command Line Parameters

<table>
<tr><th>Parameter</th><th colspan="2">Description</th></tr>
<tr><td>-? or –help</td><td colspan="2">Displays a short help page for the operation of TPMFactoryUpd. Cannot be used with any other parameter.</td></tr>
<tr><td>-info</td><td colspan="2">Displays TPM information related to TPM Firmware Update. Cannot be used with -update and -tpm12-clearownership parameter.</td></tr>
<tr><td rowspan="6">-update <update-type></td><td colspan="2">Updates a TPM with <update-type>. Possible values for <update-type> are:</td></tr>
<tr><td>tpm12-PP</td><td>TPM1.2 with Physical Presence or Deferred Physical Presence.</td></tr>
<tr><td>tpm12-takeownership</td><td>TPM1.2 with TPM ownership taken by TPMFactoryUpd.</td></tr>
<tr><td>tpm20-emptyplatformauth</td><td>TPM2.0 with platformAuth set to Empty Buffer.</td></tr>
<tr><td>config-file</td><td>Updates either a TPM1.2 or TPM2.0 to the firmware version configured in the configuration file. Requires the -config parameter.</td></tr>
<tr><td colspan="2">Cannot be used with -info and -tpm12-clearownership parameter.</td></tr>
<tr><td>-firmware <firmware-file></td><td colspan="2">Specifies the path to the firmware image file to be used for firmware update. Required if -update parameter is given with values tpm*, cannot be used with -info parameter.</td></tr>
<tr><td>-config <config-file></td><td colspan="2">Specifies the path to the configuration file to be used for firmware update. Required if –update parameter is given with value config-file, cannot be used with –info parameter. Chapter 5.2 explains the configuration file in more detail.</td></tr>
<tr><td>-log [<log-file>]</td><td colspan="2">Optional parameter. Activates logging for TPMFactoryUpd to the log file specified by <log-file>. Default value ./TPMFactoryUpd.log is used if <log-file> is not given.

<i>Note: Total path and file name length must not exceed 260 characters.</i>

<i>Note: TPM Firmware Update with logging can be slow depending on system configuration. To reduce the delay, avoid creating a log file on external/slow media.</i></td></tr>
<tr><td>-tpm12-clearownership</td><td colspan="2">Clears a TPM1.2 ownership which was taken earlier during an update with owner authorization.
Cannot be used with -info and -update parameter.</td></tr>
</table>

Parameter	Description
-access-mode <mode> <path>	Optional parameter. Sets the mode the tool should use to connect to the TPM device. Possible values for <mode> are: 1 - Memory based access (only supported on x86 based systems with PCH TPM support) 3 - Linux TPM driver (default value). The <path> option can be set to define a device path (default value: /dev/tpm0).

Passing no parameter or an invalid combination of parameters causes the help page to be shown and the tool to exit.

5.2 Configuration File

This chapter describes the configuration file which can be used with the –config <config-file> option. It allows updating the TPM to a specific firmware version without having to know the current firmware version on the TPM. It consists of sections:

```
[UpdateType]
tpm12={tpm12-pp,tpm12-takeownership}
tpm20={tpm20-emptyplatformauth}

[TargetFirmware]
version_SLB966x=<firmware_version_slb966x>
version_SLB9670=<firmware_version_slb9670>

[FirmwareFolder]
path=.
```

The following table describes the options in the configuration file.

Table 2 Configuration File Options

Section	Key	Description
UpdateType	tpm12	Configures the update option to use when updating a TPM1.2. The value can be either *tpm12-pp* or *tpm12-takeownership*. Refer to chapter 5.1 for further information on these options.
	tpm20	Configures the update option to use when updating a TPM2.0. At the moment the value can only be *tpm20-emptyplatformauth*. Refer to chapter 5.1 for further information on this option.
TargetFirmware	version_SLB966x	Configures the target firmware version that shall be installed onto a SLB 9660 or SLB 9665 TPM. The value uses same naming convention as can be found in the command line output of the -info command line option. You can either enter a TPM1.2 firmware version or a TPM2.0 firmware version. Example values: 4.40.119.0, 5.60.2677.0
	version_SLB9670	Configures the target firmware version that shall be installed onto a SLB 9670 TPM. The value uses same naming convention as can be found in the command line output of the -info

Section	Key	Description
		command line option. You can either enter a TPM1.2 firmware version or a TPM2.0 firmware version. Example values: 6.41.198.0, 7.60.2677.0
FirmwareFolder	path	Configures the relative path to the folder containing the firmware images. TPMFactoryUpd evaluates the path relative to the location of the config file and scans that folder for a firmware image matching the search criteria. TPMFactoryUpd only scans this folder; it does not scan any subfolders.

5.3 Typical Update Sequence

A typical sequence of steps to perform a factory TPM Firmware Update:

- copy TPMFactoryUpd executable to Linux system
- copy TPM firmware image file to Linux system
- execute TPMFactoryUpd with the corresponding command line options and sudo rights
- restart the system after completion of TPM Firmware Update
- clear remaining TPM ownership taken by TPMFactoryUpd (only in case of updating a TPM1.2 to TPM1.2 with owner authorization)

5.4 Sample Usage of Command Line Options

Here are some sample combinations showing the use of the command line options:

Note: 'firmware.bin' in the examples below has to be replaced with the actual firmware image file name.

5.4.1 Update a TPM2.0

To update a TPM2.0 using Platform Policy authorization, run the following command:

```
TPMFactoryUpd -update tpm20-emptyplatformauth -firmware firmware.bin
```

Sample output:

```
**********************************************************************
*    Infineon Technologies AG   TPMFactoryUpd   Ver 01.01.xxxx.00    *
**********************************************************************

     TPM update information:
     -----------------------
     Firmware valid                    :    Yes
     TPM family                        :    2.0
     TPM firmware version              :    <current_fw_version>
     Remaining updates                 :    <1...max>
     New firmware valid for TPM        :    Yes
     TPM family after update           :    1.2
     TPM firmware version after update :    <new_fw_version>
     TPM chip state after update       :    reset to factory defaults

     Preparation steps:
     TPM2.0 policy session created to authorize the update.

  DO NOT TURN OFF OR SHUT DOWN THE SYSTEM DURING THE UPDATE PROCESS!

     Updating the TPM firmware ...
     Completion: 1 %
     ...
     Completion: 100 %

     TPM Firmware Update completed successfully.
```

5.4.2 Update a TPM1.2 Using Deferred Physical Presence

To update a TPM1.2 using Deferred Physical Presence authorization, run the following command:

```
TPMFactoryUpd -update tpm12-PP -firmware firmware.bin
```

Sample output:

```
**********************************************************************
*    Infineon Technologies AG   TPMFactoryUpd   Ver 01.01.xxxx.00    *
**********************************************************************

     TPM update information:
     -----------------------
     Firmware valid                    :    Yes
     TPM family                        :    1.2
     TPM owner set                     :    No
     TPM firmware version              :    <current_fw_version>
     Remaining updates                 :    <1...max>
     New firmware valid for TPM        :    Yes
     TPM family after update           :    2.0
     TPM firmware version after update :    <new_fw_version>
     TPM chip state after update       :    reset to factory defaults

     Preparation steps:
     TPM1.2 Physical Presence not locked, Deferred Physical Presence
     preparation successful.

  DO NOT TURN OFF OR SHUT DOWN THE SYSTEM DURING THE UPDATE PROCESS!

     Updating the TPM firmware ...
     Completion: 1 %
     ...
     Completion: 100 %

     TPM Firmware Update completed successfully.
```

5.4.3 Update a TPM1.2 Using TPM Owner Authorization

To update a TPM1.2 using owner authorization, run the following command:

```
TPMFactoryUpd -update tpm12-takeownership -firmware firmware.bin
```

Sample output:

```
  **********************************************************************
  *    Infineon Technologies AG   TPMFactoryUpd   Ver 01.01.xxxx.00    *
  **********************************************************************

       TPM update information:
       -----------------------
       Firmware valid                    :    Yes
       TPM family                        :    1.2
       TPM owner set                     :    No
       TPM firmware version              :    <current_fw_version>
       Remaining updates                 :    <1...max>
       New firmware valid for TPM        :    Yes
       TPM family after update           :    2.0
       TPM firmware version after update :    <new_fw_version>
       TPM chip state after update       :    reset to factory defaults

       Preparation steps:
       TPM1.2 Ownership preparation was successful.

    DO NOT TURN OFF OR SHUT DOWN THE SYSTEM DURING THE UPDATE PROCESS!

       Updating the TPM firmware ...
       Completion: 1 %
       ...
       Completion: 100 %

       TPM Firmware Update completed successfully.
```

5.4.4 Clear ownership of a TPM1.2

To clear the TPM1.2 ownership – taken by an owner authorized update – run the following command:

```
TPMFactoryUpd -tpm12-clearownership
```

Sample output:

```
  **********************************************************************
  *    Infineon Technologies AG   TPMFactoryUpd   Ver 01.01.xxxx.00    *
  **********************************************************************

       TPM1.2 Clear Ownership:
       -------------------------------------
       Clear TPM1.2 Ownership operation completed successfully.
```

5.4.5 Update a TPM to latest firmware version

This sample usage allows updating the TPM to a specific firmware version without the caller having to know the current firmware version installed on the TPM. Select one of the provided configuration files (for example TPM20_latest.cfg or TPM12_latest.cfg) or create a custom configuration file to instruct TPMFactoryUpd to update to a specific TPM firmware version. TPMFactoryUpd will query the TPM family and TPM firmware version from the TPM and then scans the configured Firmware folder to select an appropriate .BIN file for TPM Firmware Update. TPMFactoryUpd will then run TPM Firmware Update using the selected .BIN file.

Run the following command:

```
TPMFactoryUpd -update config-file -config ../../../Firmware/TPM12_latest.cfg
```

Sample Output:

```
  **********************************************************************
  *    Infineon Technologies AG   TPMFactoryUpd   Ver 01.01.xxxx.00    *
  **********************************************************************

       TPM update information:
       -----------------------
       Firmware valid                    :    Yes
       TPM family                        :    2.0
       TPM firmware version              :    <current_fw_version>
       Remaining updates                 :    <1...max>
       New firmware valid for TPM        :    Yes
       TPM family after update           :    1.2
       TPM firmware version after update :    <new_fw_version>
       TPM chip state after update       :    reset to factory defaults

       Selected firmware image
       TPM20_<current_fw_version>_to_TPM12_<new_fw_version>.BIN


       Preparation steps:
       TPM2.0 policy session created to authorize the update.

    DO NOT TURN OFF OR SHUT DOWN THE SYSTEM DURING THE UPDATE PROCESS!

       Updating the TPM firmware ...
       Completion: 1 %
       ...
       Completion: 100 %

       TPM Firmware Update completed successfully.
```

5.4.6 Show Information about TPM and TPM Firmware

To just show information about the current TPM and its firmware, run the following command:

```
TPMFactoryUpd -info
```

Sample output for TPM2.0:

```
**********************************************************************
*    Infineon Technologies AG   TPMFactoryUpd   Ver 01.01.xxxx.00    *
**********************************************************************

     TPM information:
     ----------------
     Firmware valid                     :    Yes
     TPM family                         :    2.0
     TPM firmware version               :    <current_fw_version>
     TPM platformAuth                   :    <platform_auth>
     Remaining updates                  :    <0...max>
```

The row *TPM platformAuth* can be used to check whether TPMFactoryUpd can update the TPM2.0 with *tpm20-emptyplatformauth* option. Possible values for <platform_auth> and corresponding descriptions are listed in Table 3 below:

Table 3 <platform_auth> values

Value	Description
Empty Buffer	platformAuth is the Empty Buffer. In this state TPMFactoryUpd can be used to update the TPM2.0.
Not Empty Buffer	platformAuth is not the Empty Buffer. In this state TPMFactoryUpd cannot be used to update the TPM2.0. Instead the System Firmware can use the IFXTPMUpdate.efi UEFI driver to update the TPM2.0 (System Firmware needs to know the value of platformAuth).
Platform hierarchy disabled	The platform hierarchy is disabled. In this state TPMFactoryUpd cannot be used to update the TPM2.0. The System Firmware must enable the platform hierarchy on next reboot if TPM2.0 needs to be updated.

Sample output for TPM1.2:

```
**********************************************************************
*    Infineon Technologies AG   TPMFactoryUpd   Ver 01.01.xxxx.00    *
**********************************************************************

     TPM information:
     ----------------
     Firmware valid                     :    Yes
     TPM family                         :    1.2
     TPM firmware version               :    <current_fw_version>
     TPM enabled                        :    <Yes/No>
     TPM activated                      :    <Yes/No>
     TPM owner set                      :    <Yes/No>
     TPM deferred physical presence     :    <deferred_pp>
     Remaining updates                  :    <0...max>
```

The rows *TPM enabled, TPM activated,* and *TPM owner set* can be used to check whether TPMFactoryUpd can update the TPM1.2 with the *tpm12-takeownership* option. Preconditions for option *tpm12-takeownership* are:

- TPM enabled: Yes
- TPM activated: Yes
- TPM owner set: No

The rows *TPM deferred physical presence* and *TPM owner set* can be used to check whether TPMFactoryUpd can update the TPM1.2 with the *tpm12-PP* option. Preconditions for option *tpm12-PP* are:

- TPM owner set: No
- TPM deferred physical presence: Yes | No (Settable)

Possible values for <deferred_pp> and corresponding descriptions are listed in Table 4 below:

Table 4 <deferred_pp> values

Value	**Description**
Yes	Deferred Physical Presence is asserted in the TPM1.2. In this state TPMFactoryUpd can be used to update the TPM1.2 with the *tpm12-PP* update option.
No (Settable)	Deferred Physical Presence is not asserted in the TPM1.2. However, Physical Presence is not locked and TPMFactoryUpd is able to assert Deferred Physical Presence. In this state TPMFactoryUpd can be used to update the TPM1.2 with the *tpm12-PP* update option.
No (Not settable)	Deferred Physical Presence is not asserted in the TPM1.2. Physical Presence is locked and TPMFactoryUpd is not able to assert Deferred Physical Presence. In this state TPMFactoryUpd cannot be used to update the TPM1.2 with the *tpm12-PP update option*.

Sample output for interrupted TPM Firmware Update:

```
***********************************************************************
*    Infineon Technologies AG   TPMFactoryUpd   Ver 01.01.xxxx.00    *
***********************************************************************

     TPM information:
     ----------------
     Firmware valid                    :    No
     TPM family                        :    N/A
     TPM firmware version              :    N/A
```

5.4.7 Show Help

To explicitly show the help, run the following command:

```
TPMFactoryUpd -help
```

5.4.8 Create Log File for Debug Purposes

To create a log file of TPM Firmware Update operation for debug purposes, enable logging, for example:

```
TPMFactoryUpd -update tpm12-takeownership -firmware firmware.bin -log log.txt
```

Note: *TPM Firmware Update with logging can be slow depending on system configuration. To reduce the delay, avoid creating a log file on external/slow media.*

5.5 Return Codes

Due to the Linux return code conventions the Infineon TPM Factory Update Tool returns 0x00 in case of a successful execution and 0x01 in case of an error. The error codes specific to Infineon TPM Factory Update Tool can be divided in two categories which are listed below.

5.5.1 Tool Errors

Return codes in this category indicate application errors that always cause the execution to stop immediately and use 0x01 as return code of the program.

On application exit, a simple error message is shown on the screen while an error entry with more detailed error information is written to the log file.

All tool error return codes are listed in Table 5 below:

Table 5 Tool Error Codes

Error Code	Error Message
0xE0295001	An unexpected error occurred.
0xE0295002	Invalid command line parameter(s). *Note: Refer to section 5.1 for all possible command line options and combinations.*
0xE0295007	The TPM device is in use by another process.
0xE0295008	The application does not have the appropriate rights to access the TPM device.
0xE0295009	A setting in the configuration file is invalid.
0xE029500A	The selected command line option cannot be used with the TPM family.
0xE0295100	An internal error occurred.
0xE0295200	No connection to the TPM or TPM not found.
0xE0295500	The firmware update process returned an unexpected value.
0xE0295503	An invalid value was passed in the <firmware> command line option.
0xE0295504	The firmware image cannot be used to update the TPM.
0xE0295505	An invalid value was passed in the <log> command line option.
0xE0295506	The TPM is not an Infineon TPM.
0xE0295507	TPM2.0: PlatformAuth is not the Empty Buffer. The firmware cannot be updated.
0xE0295508	TPM2.0: The platform hierarchy is disabled. The firmware cannot be updated.
0xE0295509	The TPM does not allow further updates because the update counter is zero.
0xE029550A	The firmware update started but failed.
0xE029550B	TPM1.2: The TPM has an owner. The firmware cannot be updated.
0xE029550E	The selected <update> command line option cannot be used with the TPM family.
0xE029550F	The system must be restarted before the TPM can be updated.
0xE0295510	TPM1.2: Deferred Physical Presence is not set. The firmware cannot be updated.
0xE0295511	TPM1.2: The TPM is disabled or deactivated. The firmware cannot be updated.
0xE0295512	TPM1.2: The TPM is locked out due to dictionary attack. The firmware cannot be updated.
0xE0295513	The firmware image provided requires a newer version of this tool.
0xE0295514	The Infineon TPM chip detected is not supported by this tool.
0xE0295515	The firmware image is corrupt.
0xE0295516	The firmware image cannot be used to update this TPM (decrypt key mismatch).
0xE0295517	An invalid value was passed in the <config> command line option.
0xE0295518	Could not find a firmware image to update to the configured target firmware version.
0xE029551A	Cannot resume interrupted firmware update with option '-update config-file' because file

Error Code	Error Message
	'TPMFactoryUpd_RunData.txt' is missing.
0xE0295522	TPM1.2: The owner secret does not match.
0xE0295523	TPM1.2: The TPM has no owner.
0xE0295528	An invalid value was passed in the <access-mode> command line option.
0xE0295529	The TPM2.0 is in failure mode. TPM firmware update is not possible. Restart the system and try again.

5.5.2 TPM Errors

The error code in this category indicates that an error has been returned by the TPM. This also implies that communication with the TPM was possible, but execution of the actual TPM command has failed.

A TPM error causes the application to exit with return code 0x01. A detailed error message is shown on the screen and a log entry is written, too.

The general application return code indicating a TPM error is listed below:

Table 6

Error Code	Error Message
0xE0295300	A TPM error occurred.

More specific TPM error information can be obtained from the provided error details.

6 References

[1] "SLB 9660 TPM1.2 Basic Platform Manufacturer Guideline, CONFIDENTIAL, Distribution under NDA only".

[2] "SLB 9670 TPM1.2 Basic Platform Manufacturer Guideline, CONFIDENTIAL, Distribution under NDA only".

[3] "TPM2.0 User Guidance, CONFIDENTIAL, Distribution under NDA only".

Revision History

Major changes since revision 1.0

Page or Reference	Description of change
5.4	TPMFactoryUpd displays the number of remaining updates
5.4	TPMFactoryUpd displays when chip is set to factory defaults
3.3, 5.4, 5.5	TPMFactoryUpd is able to clear a TPM1.2 ownership taken earlier by the tool
2	Updated the operating environment

Major changes since revision 1.4

Page or Reference	Description of change
3.1.1, 3.1.3, 3.2.2	Updated pictures
3.1.2	Added Attention note to EmptyBuffer usage
All	Use new document template
All	Added Linux relevant information
5.3	TPMFactoryUpd displays the value of deferred physical presence for TPM1.2 TPMFactoryUpd displays platformAuth state for TPM2.0
5.4.1	Added additional Error Codes
All	Added “-update config-file” option

Edition 2015-09-01

Published by
Infineon Technologies AG
81726 Munich, Germany

Do you have a question about this document?

Email: erratum@infineon.com

Document reference

IMPORTANT NOTICE

The information contained in this application note is given as a hint for the implementation of the product only and shall in no event be regarded as a description or warranty of a certain functionality, condition or quality of the product. Before implementation of the product, the recipient of this application note must verify any function and other technical information given herein in the real application. Infineon Technologies hereby disclaims any and all warranties and liabilities of any kind (including without limitation warranties of non-infringement of intellectual property rights of any third party) with respect to any and all information given in this application note.

The data contained in this document is exclusively intended for technically trained staff. It is the responsibility of customer's technical departments to evaluate the suitability of the product for the intended application and the completeness of the product information given in this document with respect to such application.

For further information on the product, technology, delivery terms and conditions and prices please contact your nearest Infineon Technologies office (**www.infineon.com**).

WARNINGS

Due to technical requirements products may contain dangerous substances. For information on the types in question please contact your nearest Infineon Technologies office.

Except as otherwise explicitly approved by Infineon Technologies in a written document signed by authorized representatives of Infineon Technologies, Infineon Technologies' products may not be used in any applications where a failure of the product or any consequences of the use thereof can reasonably be expected to result in personal injury.