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

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 4) and about the usage of Infineon TPM Factory Update Tool (see chapter 7).

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 6 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 (only for SLB 9672)

Infineon TPM Factory Update Tool supports updating the firmware of a SLB 9672 TPM from TPM2.0 to TPM2.0.

In addition, Infineon TPM Factory Update Tool supports a new command line parameter -setmode to switch the TPM into firmware update, firmware recovery or into TPM operational mode again (see 7.1).

Attention: ***The number of firmware update attempts is limited. The TPM supports an overall firmware update counter and a counter for updates onto the same firmware version. For the exact numbers supported by a particular TPM model please consult the TPM documentation or contact your local Infineon representative. Once one of the limits 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 command before attempting actual firmware update.***

Attention: ***After performing TPM Firmware Update or Recovery some postconditions must be fulfilled in order to get the TPM back into an operational state. These conditions are listed in chapter 3.1.4.***

3.1 TPM2.0 Firmware Update or Firmware Recovery

This chapter describes preconditions and scenarios for updating the TPM firmware or for recovering a corrupt TPM firmware.

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 for example can authorize a TPM 2.0 Firmware Update by setting the Platform Policy which needs an Empty Buffer platformAuth (see 3.1.2.1) for manufacturing or service environments.

Chapter 3.1.2 gives information about the different update scenarios and the used authorization possibilites.

The following Figure 1 describes the actions the Infineon TPM Factory Update Tool performs to update the TPM 2.0 Firmware for Empty Buffer platformAuth.

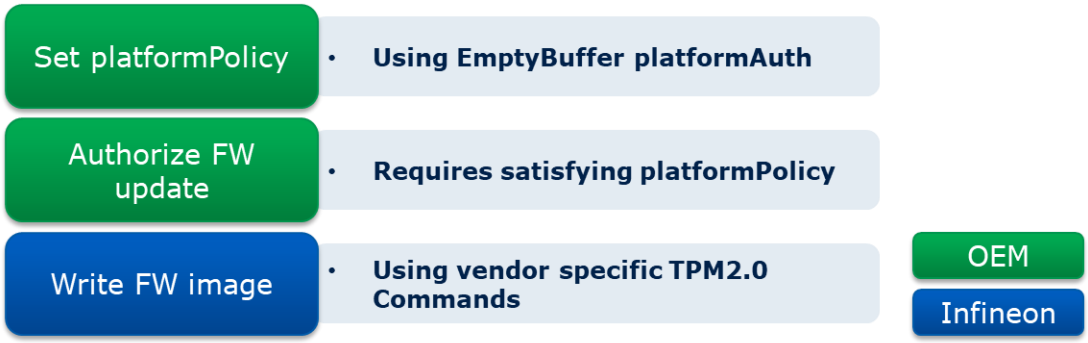

Figure 1: High Level Actions (only for SLB 9672)

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.

However, if Platform Policy is already set by the platform BIOS/firmware, the Infineon TPM Factory Update Tool will create or use a Policy Session (utilizing SHA2-256 algorithm) for the update type tpm20-platformpolicy depending on its parameter usage:

- No parameter (default):
  Calling TPM2_PolicyCommandCode(TPM_CC_FieldUpgradeStartVendor)
- Parameter -policyfile:
  Calling TPM2_PolicyOR having one option for
  TPM2_PolicyCommandCode(TPM_CC_FieldUpgradeStartVendor)
- Parameter -policyhandle:
  Using external created policy session including
  TPM2_PolicyCommandCode(TPM_CC_FieldUpgradeStartVendor)

The resulting SHA2-256 policy digest of TPM2_PolicyCommandCode(TPM_CC_FieldUpgradeStartVendor) that can be used to set the TPM platform policy or can be used for TPM2_PolicyOR command is:
652351CB9FE7D86EB244A95E5AD4DDB79C1138C0BFE15B1664F69F5E74C94539

3.1.2 Update Scenarios

This chapter describes the different update scenarios.

3.1.2.1 Using platformAuth set to Empty Buffer

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.***

The scenario for TPM2.0 to TPM2.0 firmware update is shown in Figure 2 and is normally used to update a TPM with a newer firmware version. In addition, Infineon TPM Factory Update Tool also supports updating a TPM with the same firmware version as currently running on the TPM (only for SLB 9672).

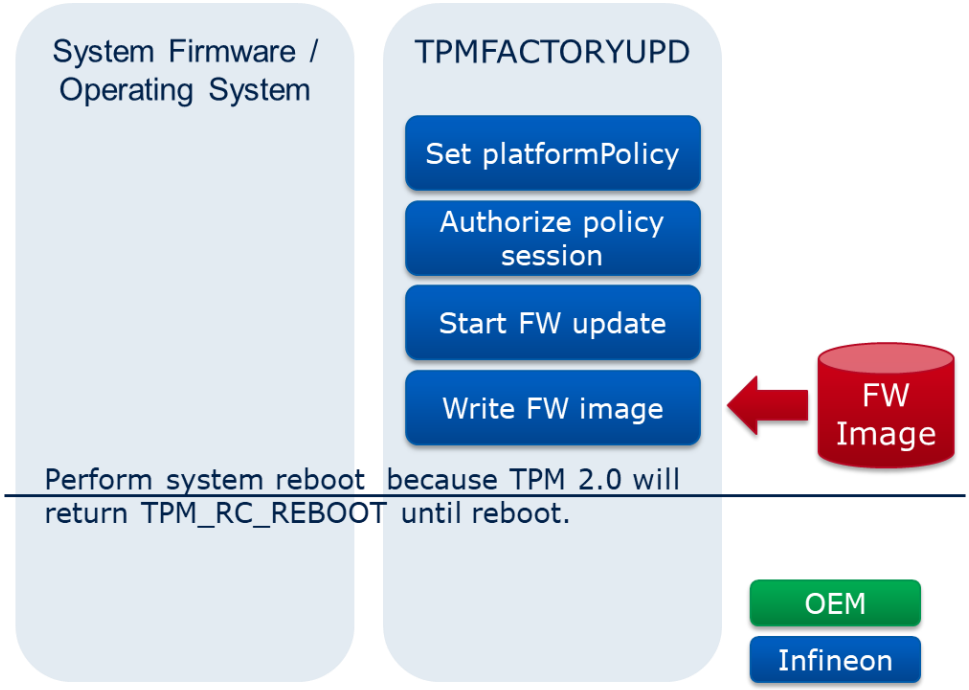

Figure 2: TPM2.0 to TPM2.0 Firmware Update (only for SLB 9672)

3.1.2.2 Using external policy session handle

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

- Platform hierarchy is enabled
- Policy command code for TPM2_FieldUpgradeStartVendor is used within the policy session
- Policy session handle is available

Compared to the scenario as shown in Figure 2, platformAuth does not need to be Empty Buffer and the authorization session is generated outside of the tool and its handle must be used with Infineon TPM Factory Update Tool to update the firmware with the supplied policy session from TPM2.0 to TPM2.0. It also supports updating a TPM with the same firmware version as currently running on the TPM (only for SLB 9672).

3.1.2.3 Using platform policy (with policy command code only)

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

- Platform hierarchy is enabled
- Platform policy is set with the digest only of policy command code for TPM2_FieldUpgradeStartVendor

Compared to the scenario as shown in Figure 2, platformAuth does not need to be Empty Buffer and the platform policy must be set outside of the tool. Since the policy digest of policy command code for TPM2_FieldUpgradeVendor is static, the Infineon TPM Factory Update Tool updates the firmware with a corresponding internal policy session from TPM2.0 to TPM2.0. It also supports updating a TPM with the same firmware version as currently running on the TPM (only for SLB 9672).

3.1.2.4 Using platform policy (with policy file)

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

- Platform hierarchy is enabled
- Platform policy is set with the digest of TPM2_PolicyOR having one option for policy command code for TPM2_FieldUpgradeStartVendor
- Policy file containing policy digests for TPM2_PolicyOR including the digest of policy command code for TPM2_FieldUpgradeStartVendor

Compared to the scenario as shown in Figure 2, platformAuth does not need to be Empty Buffer and the platform policy must be set outside of the tool. The policy file must contain all policy digests to fullfil the platform policy set for TPM2_PolicyOR. The Infineon TPM Factory Update Tool updates the firmware with a corresponding internal policy session from TPM2.0 to TPM2.0. It also supports updating a TPM with the same firmware version as currently running on the TPM (only for SLB 9672).

3.1.3 Recover from TPM in non-operational mode

In case the TPM is in “Non-Operational mode” (interrupted TPM Firmware Update or TPM Firmware Recovery was triggered), the TPM will support only a limited number of TPM2.0 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 resolving the TPM “Non-operational mode” is done immediately.

Attention: ***It must be ensured to use the correct TPM firmware image. Either use the same TPM firmware image that has been used to start the TPM Firmware Update process or in case of TPM Firmware Recovery use the currently loaded firmware version.***

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.*

The scenario for interrupted TPM Firmware Update or TPM Firmware Recovery is shown in Figure 3.

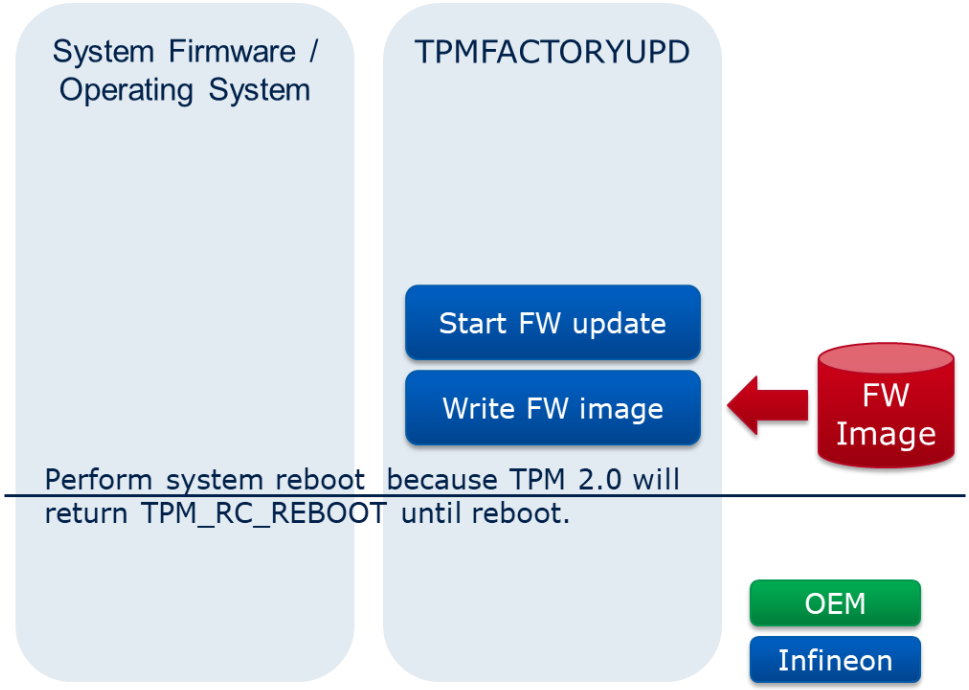

Figure 3: Interrupted TPM Firmware Update or Firmware Recovery

3.1.4 Postconditions

In case of any TPM Firmware Update or Firmware Recovery 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.

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.***

4 TPM Firmware Update Overview (except SLB 9672)

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 4.1 and 4.2.

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 command 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 4.4.***

4.1 TPM2.0 Firmware Update

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

4.1.1 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 for example can authorize a TPM 2.0 Firmware Update by setting the Platform Policy which needs an Empty Buffer platformAuth (see 4.1.2.1) for manufacturing or service environments.

Chapter 4.1.2 gives information about the different update scenarios and the used authorization possibilites.

The following Figure 4 describes the actions the Infineon TPM Factory Update Tool performs to update the TPM 2.0 Firmware for Empty Buffer platformAuth.

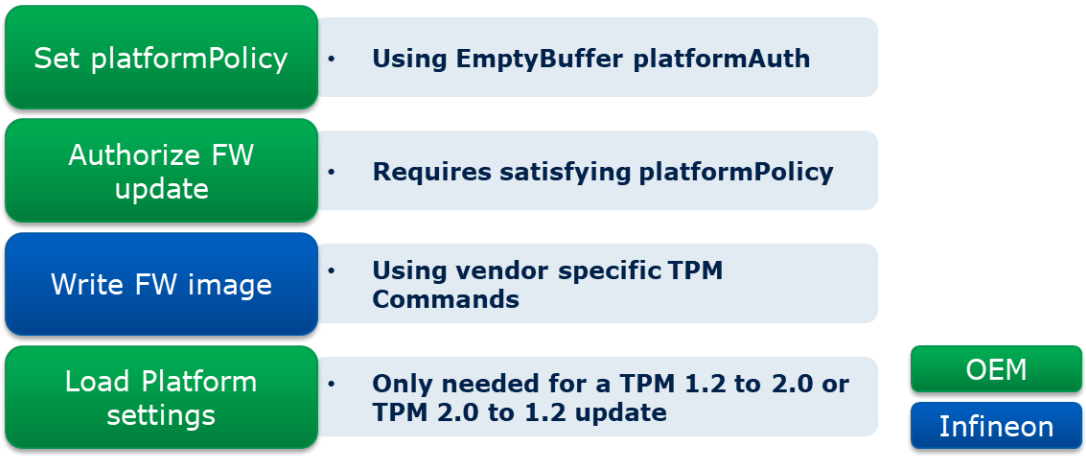

Figure 4: High Level Actions

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.

However, if Platform Policy is already set by the platform BIOS/firmware, the Infineon TPM Factory Update Tool will create or use a Policy Session (utilizing SHA2-256 algorithm) for the update type tpm20-platformpolicy depending on its parameter usage:

- No parameter (default):
  Calling TPM2_PolicyCommandCode(TPM_CC_FieldUpgradeStartVendor)
- Parameter -policyfile:
  Calling TPM2_PolicyOR having one option for
  TPM2_PolicyCommandCode(TPM_CC_FieldUpgradeStartVendor)
- Parameter -policyhandle:
  Using external created policy session including
  TPM2_PolicyCommandCode(TPM_CC_FieldUpgradeStartVendor)

The resulting SHA2-256 policy digest of TPM2_PolicyCommandCode(TPM_CC_FieldUpgradeStartVendor) that can be used to set the TPM platform policy or can be used for TPM2_PolicyOR command is:
652351CB9FE7D86EB244A95E5AD4DDB79C1138C0BFE15B1664F69F5E74C94539

4.1.2 Update Scenarios

This chapter describes the different update scenarios.

4.1.2.1 Using platformAuth set to Empty Buffer

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.***

The scenario for TPM2.0 to TPM2.0 firmware update in Figure 5 and for TPM2.0 to TPM1.2 firmware update is shown in TPM2.0 to TPM2.0 Firmware Update Figure 6.

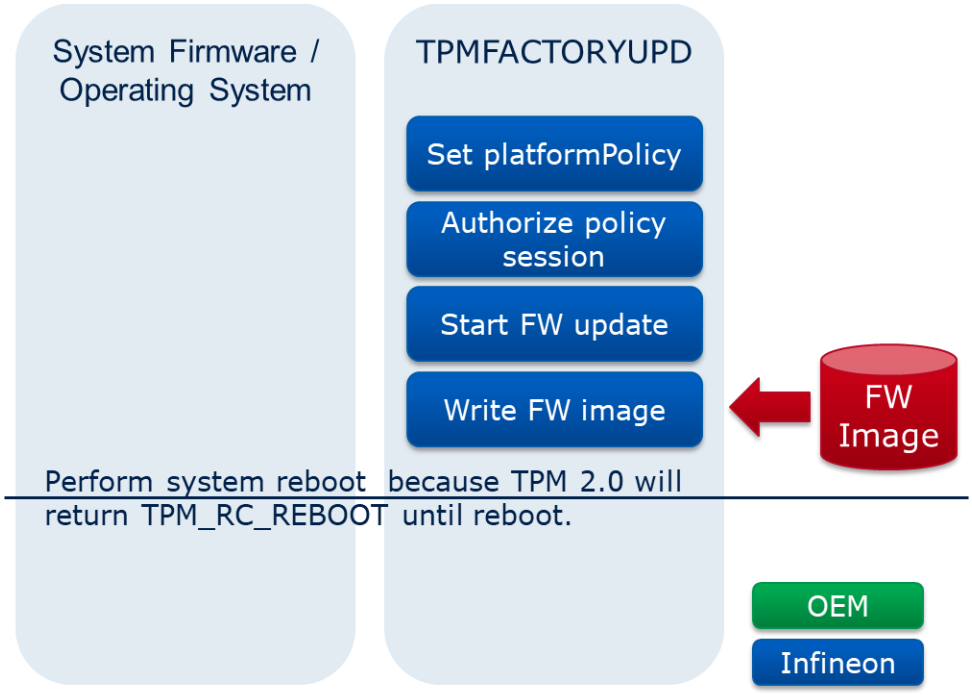

Figure 5: TPM2.0 to TPM2.0 Firmware Update

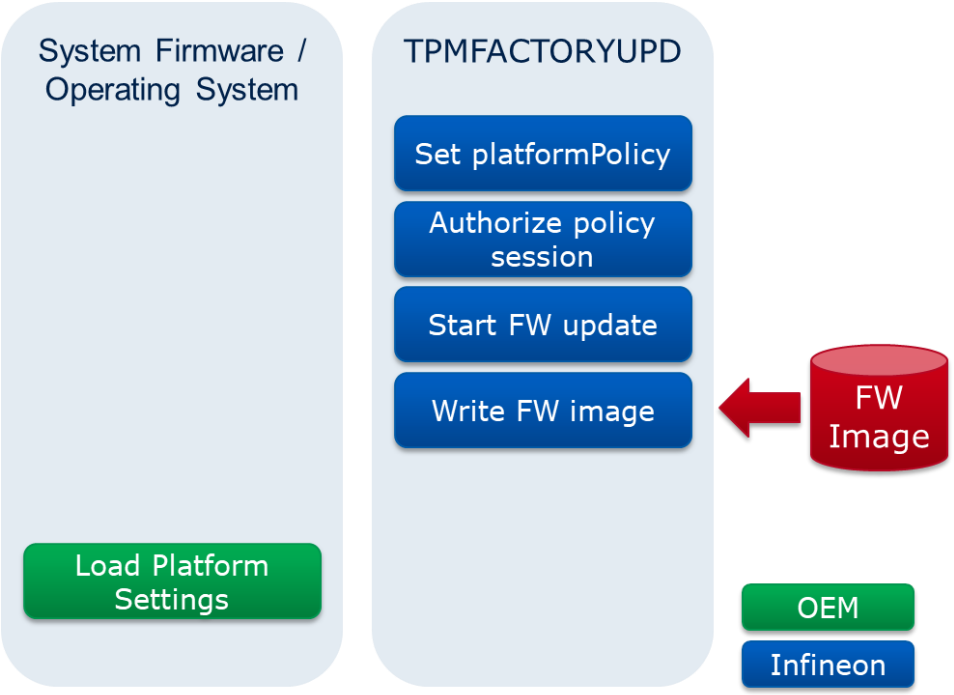

Figure 6: TPM2.0 to TPM1.2 Firmware Update

4.1.2.2 Using external policy session handle

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

- Platform hierarchy is enabled
- Policy command code for TPM2_FieldUpgradeStartVendor used within policy session
- Policy session handle is available

Compared to the scenario as shown in Figure 5 or Figure 6, platformAuth does not need to be Empty Buffer and the authorization session is generated outside of the tool and its handle must be used with Infineon TPM Factory Update Tool to update the firmware with the supplied policy session from TPM2.0.

4.1.2.3 Using platform policy (with policy command code only)

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

- Platform hierarchy is enabled
- Platform policy is set with the digest only of policy command code for TPM2_FieldUpgradeStartVendor

Compared to the scenario as shown in Figure 5 or Figure 6, platformAuth does not need to be Empty Buffer and the platform policy must be set outside of the tool. Since the policy digest of policy command code for TPM2_FieldUpgradeVendor is static, the Infineon TPM Factory Update Tool updates the firmware with a corresponding internal policy session from TPM2.0.

4.1.2.4 Using platform policy (with policy file)

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

- Platform hierarchy is enabled
- Platform policy is set with the digest of TPM2_PolicyOR having one option for policy command code for TPM2_FieldUpgradeStartVendor
- Policy file containing policy digests for TPM2_PolicyOR including the digest of policy command code for TPM2_FieldUpgradeStartVendor

Compared to the scenario as shown in Figure 5 or Figure 6, platformAuth does not need to be Empty Buffer and the platform policy must be set outside of the tool. The policy file must contain all policy digests to fullfil the platform policy set for TPM2_PolicyOR. The Infineon TPM Factory Update Tool updates the firmware with a corresponding internal policy session from TPM2.0.

4.2 TPM1.2 Firmware Update

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

4.2.1 Preconditions

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

4.2.1.1 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.***

4.2.1.2 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)

4.2.2 Update Scenarios

This chapter describes the update scenarios using different authorization values.

4.2.2.1 Using Deferred Physical Presence Authorization

The scenario using DPP authorization for TPM1.2 to TPM2.0 firmware update is shown in Figure 7 and for TPM1.2 to TPM1.2 firmware update in Figure 8.

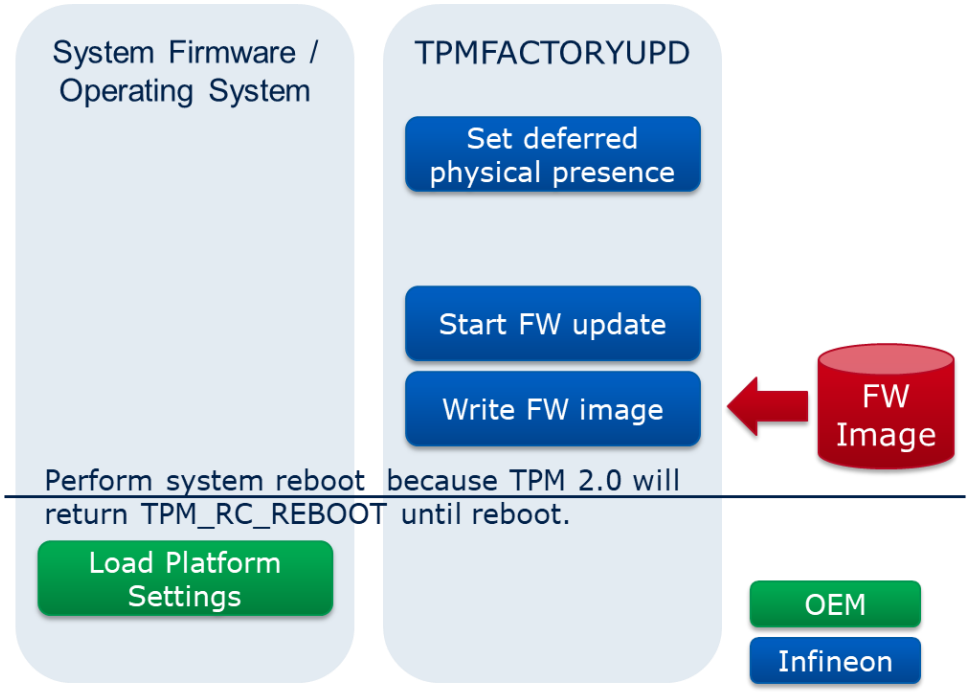

Figure 7: TPM1.2 to TPM2.0 Firmware Update using Deferred Physical Presence authorization

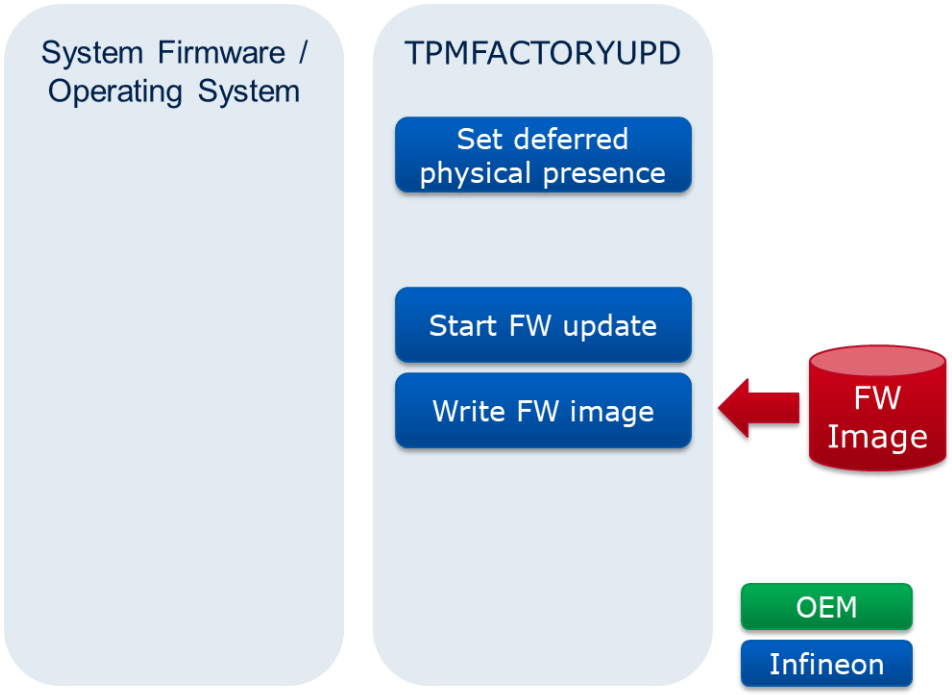

Figure 8: TPM1.2 to TPM1.2 Firmware Update using Deferred Physical Presence authorization

4.2.2.2 Using TPM Owner Authorization

The scenario using TPM Owner authorization for TPM1.2 to TPM2.0 firmware update is shown in Figure 9 and for TPM1.2 to TPM1.2 firmware update in Figure 10.

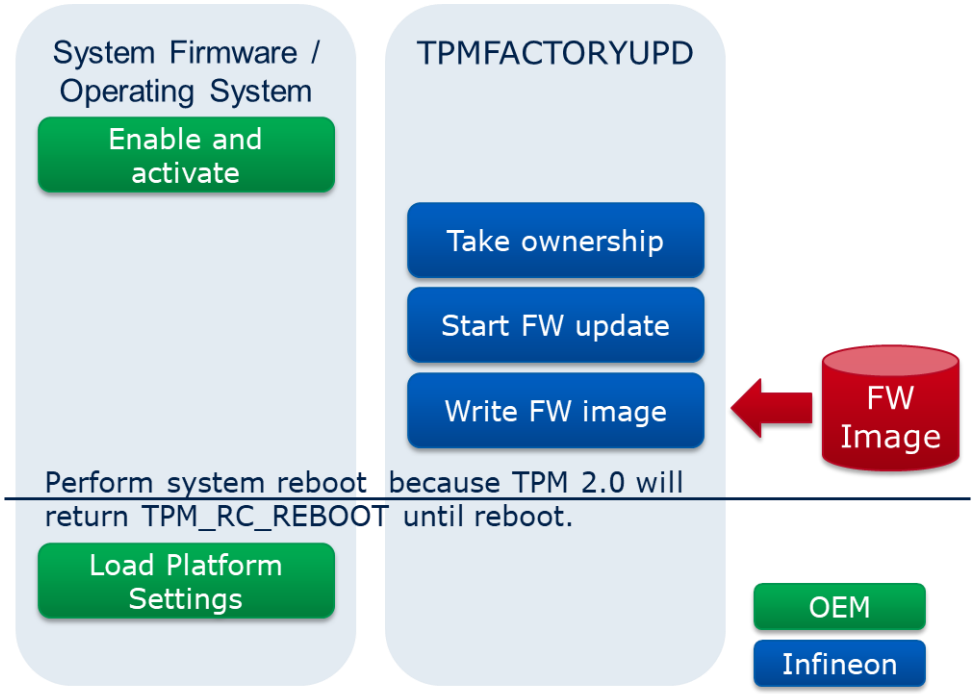

Figure 9: TPM1.2 to TPM2.0 Firmware Update using TPM Owner authorization

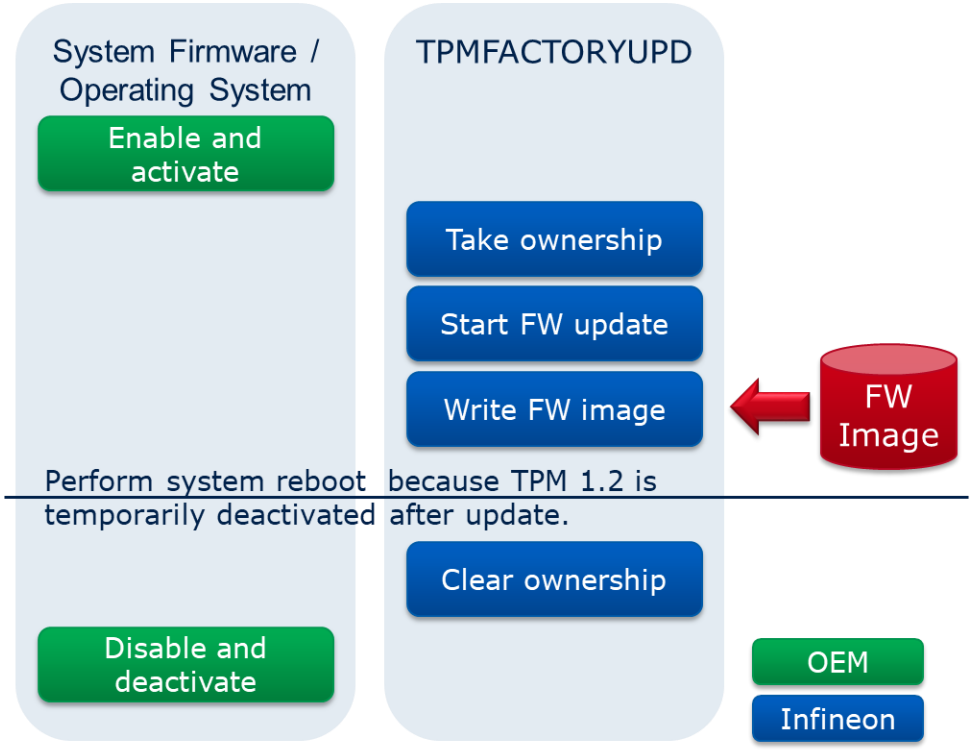

Figure 10: TPM1.2 to TPM1.2 Firmware Update using TPM Owner authorization

4.3 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 7.4.2).

4.3.1 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], [3] for your TPM Model which can be requested from your local Infineon representative.

4.3.2 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 [4] which can be requested from your local Infineon representative and refer to chapter 7.3 in TCG TPM v2.0 Provisioning Guidance [5].

4.4 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 7.4.10).

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).***

4.5 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.

TPM Firmware Update Overview (except SLB 9672)

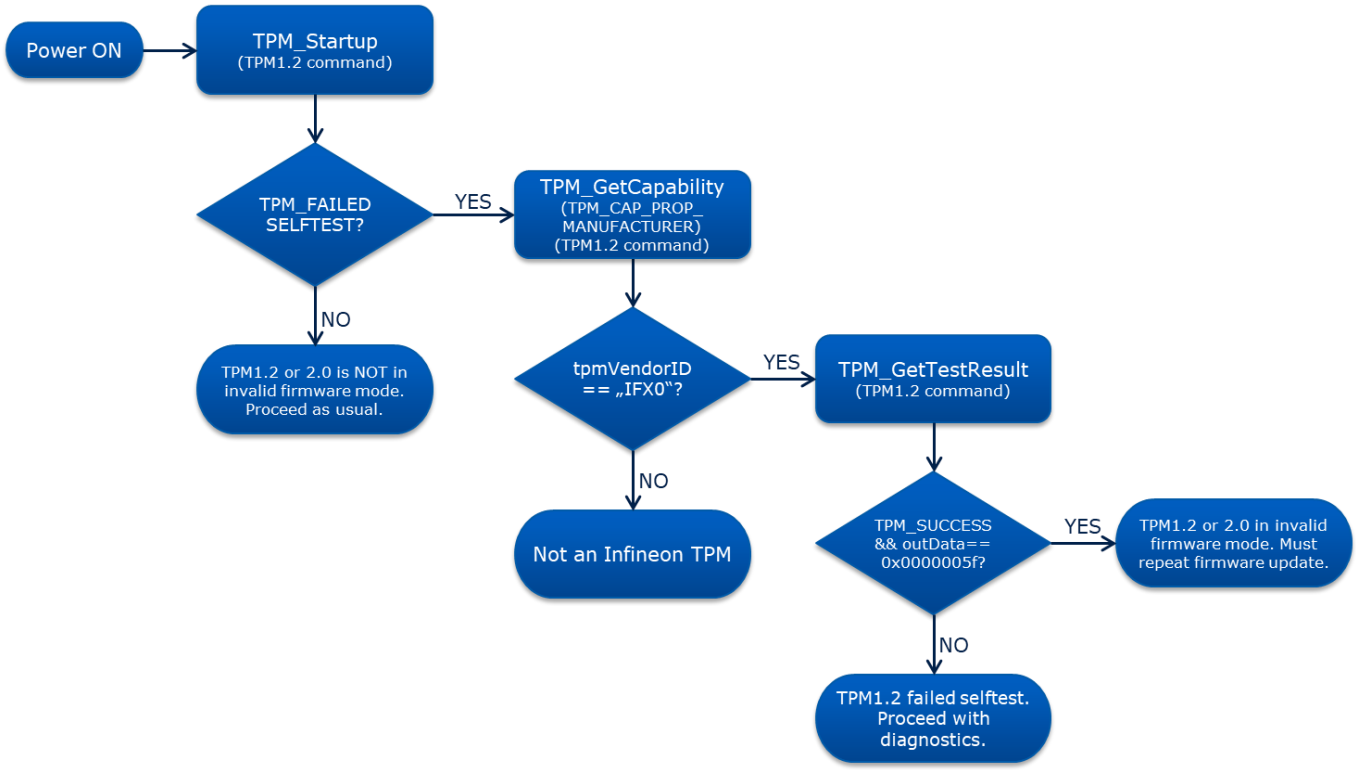

Figure 11: Invalid Firmware Mode Detection

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.*

5 Naming of Firmware Images

Firmware image files use a specific naming scheme for each type of image:

- The Combined firmware update and recovery image (only for SLB 9672) allows updating to a specific target firmware version from older and same firmware version and is also intended to be used for TPM Firmware Recovery
- The Single source image specifically allows only a single firmware version to be updated to the current one
- The Multi source image allows up to eight compatible firmware versions to be updated to the current one

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).

5.1 Combined firmware update and recovery images (only for SLB 9672)

Combined firmware update and recovery images are using the following naming scheme:

[Target]_[Version]_[Revision].bin

Placeholder values:

- Target = { TPM20 }
- Version = firmware version of firmware (for example: 1.23.456.0)
- Revision = revision number (for example R1, R2)

For example a firmware image file could be named TPM20_1.23.456.0_R1.bin. This would mean that the firmware image file would update a TPM2.0 with a lower minor version (e.g. 1.22.345.0) or with the same version to a TPM2.0 with firmware version 1.23.456.0. The same firmware image file shall be used as TPM Firmware Recovery image.

5.2 Single source images

Single source firmware image files use the following naming scheme:

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

Placeholder 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.

5.3 Multi source images

Multi source firmware image files use the following naming scheme:

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

Placeholder values:

- Source = { TPM12, TPM20 }
- Target = { TPM12, TPM20 }
- VersionRange = compatible major including a range of minor versions of the firmware without buildnumbers(for example: 1.23-45)
- Version = firmware version of firmware (for example: 2.34.1337.0)

For example a firmware image file could be named TPM12_1.23-45_to_TPM20_2.34.1337.0.bin. This would mean that the firmware image file would update any TPM1.2 matching the major version of '1' and having the minor version within the closed interval [23, 45] to a TPM2.0 with firmware version 2.34.1337.0.

6 Building the Tool

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

6.1 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.

6.2 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 7.1 and 7.5 for more information about the usage and the tools return codes.

7 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.

7.1 Command Line Parameters

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

Table 1 Command Line Parameters

Parameter	Description	
-? or -help	Displays a short help page for the operation of TPMFactoryUpd. Cannot be used with any other parameter.	
-info	Displays TPM information related to TPM Firmware Update. Cannot be used with -policyhandle, -update, -firmware, -config, -tpm12-clearownership, -setmode or -force parameter.	
-update <update-type>	Updates a TPM with <update-type>. Possible values for <update-type> are:	
	tpm12-PP	Updates an unowned TPM1.2 with Physical Presence or Deferred Physical Presence.
	tpm12-takeownership	Updates an unowned TPM1.2 by first taking TPM ownership. TPMFactoryUpd uses a constant owner authorization value (SHA-1 hash of password “12345678”). Optionally the -ownerauth parameter can be provided to override the default owner authorization value with an owner authorization file.
	tpm12-ownerauth	Updates an owned TPM1.2 with TPM owner authorization provided in owner authorization file. Requires the -ownerauth parameter.
	tpm20-emptyplatformauth	Updates a TPM2.0 with platformAuth set to Empty Buffer.
	tpm20-platformpolicy	Updates a TPM2.0 with an already set platform policy. Use optional parameters -policyhandle for and external created policy session or -policyfile for a configuration file with policy digests. Without paramter the default policy behavior is used.
	config-file	Updates either a TPM1.2 or TPM2.0 to the firmware version configured in the configuration file. Requires the -config parameter.
	Cannot be used with -info, -tpm12-clearownership or -setmode parameter.	
-firmware <firmware-file>	Specifies the path to the firmware image file to be used for firmware update. Required if -update parameter is given with values tpm*.	

<table>
<tr><th>Parameter</th><th>Description</th></tr>
<tr><td>-config <config-file></td><td>Specifies the path to the configuration file to be used for firmware update. Required if -update parameter is given with value config-file. Chapter 7.2 explains the configuration file in more detail.</td></tr>
<tr><td>-ownerauth</td><td>Specifies the path to the file containing the owner authorization value (e.g. owner password as SHA-1 hash). The file must be binary coded with 20 bytes in size. Required if -update parameter is given with value tpm12-ownerauth.</td></tr>
<tr><td>-policyhandle <handle></td><td>Specifies a policy session handle as a hexadecimal value.
Requires -update parameter with update type tpm20-platformpolicy.
Cannot be used with -policyfile, -info and -setmode parameter.</td></tr>
<tr><td>-policyfile <policyfile></td><td>Specifies a policy file with policy digests supporting more complex platform policies having different options in authorizations.
Requires -update parameter with update type tpm20-platformpolicy.
Cannot be used with -policyhandle, -info and -setmode parameter.</td></tr>
<tr><td>-log [<log-file>]</td><td>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.

Note: Total path and file name length must not exceed 260 characters.

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.</td></tr>
<tr><td>-tpm12-clearownership</td><td>Clears a TPM1.2 ownership which was taken earlier during an update with owner authorization. TPMFactoryUpd uses a constant owner authorization value (SHA-1 hash of password “12345678”). Optionally the -ownerauth parameter can be provided to override the default owner authorization value with an owner authorization file.
Cannot be used with -policyhandle, -policyfile, -info, -update, -firmware, -config, -setmode or -force parameter.</td></tr>
<tr><td>-setmode <mode></td><td>Switch into firmware update, firmware recovery or operational mode for testing purposes. Possible values for <mode> are:
<table>
<tr><td>tpm20-fwupdate</td><td>Switch to firmware update mode. Requires the -firmware parameter.</td></tr>
<tr><td>tpm20-fwrecovery</td><td>Switch to firmware recovery mode.</td></tr>
<tr><td>tpm20-operational</td><td>Switch back to TPM operational mode.</td></tr>
</table>
Cannot be used with -policyhandle, -policyfile, -info, -update, - tpm12-clearownership,
-config or -force parameter.</td></tr>
<tr><td>-force</td><td>Allows a TPM Firmware Update onto the same firmware version when used with -update parameter.
Cannot be used with -info, -tpm12-clearownership or -setmode parameter.</td></tr>
<tr><td>-access-mode <mode> <path></td><td>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)</td></tr>
</table>

Parameter	Description
	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.

7.2 Configuration Files

7.2.1 Configuration File for TPM firmware update

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=<firmware_version>
version_FW15=< firmware_image_filename>
version_SLB9645=<firmware_version_slb9645>
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 7.1 for further information on these options.
	tpm20	Configures the update option to use when updating a TPM2.0. The value can be either *tpm20-emptyplatformauth* or *tpm20-platformpolicy*. Refer to chapter 7.1 for further information on this option.
TargetFirmware	version	Configures the target firmware version that shall be installed onto the TPM. ***Attention:*** ***You can add either the "version" key or one or more "version_*" keys to the configuration file. Use "version_*" keys if you want to handle more than one TPM model or Firmware entry in the same factory script.***

Section	Key	Description
		TPMFactoryUpd will not process configuration files containing both "version" and "version_*" keys.
	version_FW15	Configures the firmware image name (and **not** the target firmware version) that shall be installed onto a SLB 9672 TPM with major firmware version "15". An example of a valid image name looks like TPM20_15.20.15686.0_R1.BIN (see also 5.1)
	version_FW<n>	Configures the firmware image name (and **not** the target firmware version) that shall be installed onto a TPM with major firmware version "n".
	version_SLB9645	Configures the target firmware version that shall be installed onto a SLB 9645 TPM. The value uses same naming convention as can be found in the command line output of the -info command line option. You can enter a TPM1.2 firmware version.
	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 command line option. You can either enter a TPM1.2 firmware version or a TPM2.0 firmware version. Example values: 6.43.243.0, 7.85.4555.0
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.

7.2.1 Configuration File for firmware update with policy file (TPM2.0 only)

This chapter describes the configuration file which can be used with the -policyfile <policyfile> option together with update type tpm20-platformpolicy. It allows updating the TPM2.0 to a specific firmware version with an already set platform policy by the platform BIOS/firmware.
At least two and maximum 8 policy digests must be defined in the policy file.
The numbering of the entries must start from 1, must be ascending and without gaps. Not used policy digest options must be removed from the policy file and the order must match the order used for TPM2_PolicyOR command. The policy digest allowing TPM Firmware Update can be at any position.

In the example below, the `PolicyDigest1` entry contains the SHA2-256 policy digest of policy command code for TPM2_FieldUpgradeStartVendor.
All other digest values have dummy values (representing no real policy digests).

```
[POLICYOR_TPMFWUPDATE]

PolicyDigest1=652351CB9FE7D86EB244A95E5AD4DDB79C1138C0BFE15B1664F69F5E74C94539
```

PolicyDigest2=2222222222222222222222222222222222222222222222222222222222222222

PolicyDigest3=3333333333333333333333333333333333333333333333333333333333333333

PolicyDigest4=4444444444444444444444444444444444444444444444444444444444444444

PolicyDigest5=5555555555555555555555555555555555555555555555555555555555555555

PolicyDigest6=6666666666666666666666666666666666666666666666666666666666666666

PolicyDigest7=7777777777777777777777777777777777777777777777777777777777777777

PolicyDigest8=8888888888888888888888888888888888888888888888888888888888888888

7.3 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 superuser privileges
- 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)

7.4 Example Usage of Command Line Options

This chapter contains some examples showing the use of the command line parameters:

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

7.4.1 Show Information about TPM and TPM Firmware

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

```
TPMFactoryUpd -info
```

Example output for TPM2.0, (e.g. SLB 9672):

```
*******************************************************************
*    Infineon Technologies AG   TPMFactoryUpd   Ver 02.00.xxxx.00    *
*******************************************************************

     TPM information:
     ----------------
     TPM family                          :    2.0
     TPM firmware version                :    <current_fw_version>
     TPM firmware recovery support       :    <Yes/No>
     TPM firmware valid                  :    <Yes/No>
     TPM operation mode                  :    Operational
     TPM platformAuth                    :    <platform_auth>
     Remaining updates                   :    <0...max>
     Remaining updates (same version)    :    <0...max>
```

The row *TPM platformAuth* can be used to check whether TPMFactoryUpd can update the TPM2.0 with *tpm20-emptyplatformauth* or *tpm20-platformpolicy* 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 with *tpm20-emptyplatformauth* option.
Not Empty Buffer	platformAuth is not the Empty Buffer. In this state TPMFactoryUpd can be used to update the TPM2.0 with *tpm20-platformpolicy* option.
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.

Example output for TPM1.2, SLB 9670:

```
*********************************************************************
*    Infineon Technologies AG   TPMFactoryUpd   Ver 02.00.xxxx.00    *
*********************************************************************

     TPM information:
     ----------------
     TPM family                          :    1.2
     TPM firmware version                :    <current_fw_version>
     TPM firmware recovery support       :    <Yes/No>
     TPM firmware valid                  :    <Yes/No>
     TPM operation mode                  :    Operational
     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.

Value	Description
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*.

Example output for interrupted TPM Firmware Update (e.g. for SLB 9670):

```
*********************************************************************
*    Infineon Technologies AG   TPMFactoryUpd   Ver 02.00.xxxx.00    *
*********************************************************************

     TPM information:
     ----------------
     TPM family                        :    N/A
     TPM firmware version              :    N/A
     TPM firmware valid                :    No
     TPM operation mode                :    Firmware update
     Remaining updates                 :    <1...max>
```

Example output for interrupted TPM Firmware Update (e.g. for SLB 9672):

```
*********************************************************************
*    Infineon Technologies AG   TPMFactoryUpd   Ver 02.00.xxxx.00    *
*********************************************************************

     TPM information:
     ----------------
     TPM family                        :    2.0
     TPM firmware version              :    <current_fw_version>
     TPM firmware recovery support     :    Yes
     TPM firmware valid                :    No
     TPM operation mode                :    Firmware update (0x02)
     TPM platformAuth                  :    N/A
     Remaining updates                 :    <1...max>
     Remaining updates (same version)  :    <1...max>
```

7.4.2 Update a TPM2.0 with platformAuth set to Empty Buffer

To update a TPM2.0 using Platform Policy authorization with platformAuth set to Empty Buffer, run the following command:

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

Example output (e.g. for SLB 9672):

```
*************************************************************************
*    Infineon Technologies AG   TPMFactoryUpd   Ver 02.00.xxxx.00     *
*************************************************************************

     TPM update information:
     -----------------------
     TPM family                          :    2.0
     TPM firmware version                :    <current_fw_version>
     TPM firmware valid                  :    Yes
     TPM operation mode                  :    Operational
     TPM platformAuth                    :    Empty Buffer
     Remaining updates                   :    <1...max>
     Remaining updates (same version)    :    <1...max>
     New firmware valid for TPM          :    Yes
     TPM family after update             :    2.0
     TPM firmware version after update   :    <new_fw_version>

     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: 0 %
     ...
     Completion: 100 %
     TPM Firmware Update completed successfully.

A system restart is required before the TPM can enter operational mode again.
```

7.4.3 Update a TPM2.0 with an external policy session handle

To update a TPM2.0 using an external created policy session (see 3.1.2.2 or 4.1.2.2), run the following command:

```
TPMFactoryUpd -update tpm20-platformpolicy -policyhandle 03000000 -firmware
firmware.bin
```

Example output (e.g. for SLB 9672):

```
*************************************************************************
*    Infineon Technologies AG   TPMFactoryUpd   Ver 02.00.xxxx.00     *
*************************************************************************

     TPM update information:
     -----------------------
     TPM family                          :    2.0
     TPM firmware version                :    <current_fw_version>
     TPM firmware valid                  :    Yes
     TPM operation mode                  :    Operational
     TPM platformAuth                    :    Not Empty Buffer
     Remaining updates                   :    <1...max>
     Remaining updates (same version)    :    <1...max>
     New firmware valid for TPM          :    Yes
     TPM family after update             :    2.0
     TPM firmware version after update   :    <new_fw_version>

     Preparation steps:
     Skipped

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

     Updating the TPM firmware ...
     Completion: 0 %
     ...
     Completion: 100 %
     TPM Firmware Update completed successfully.

A system restart is required before the TPM can enter operational mode again.
```

7.4.4 Update a TPM2.0 with already set platform policy (using policy command code)

To update a TPM2.0 using an alredy set platform policy with policy command code (see 3.1.2.3 or 4.1.2.3), run the following command:

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

Example output (e.g. for SLB 9672):

```
*************************************************************************
*    Infineon Technologies AG   TPMFactoryUpd   Ver 02.00.xxxx.00     *
*************************************************************************

     TPM update information:
     -----------------------
     TPM family                          :    2.0
     TPM firmware version                :    <current_fw_version>
     TPM firmware valid                  :    Yes
     TPM operation mode                  :    Operational
     TPM platformAuth                    :    Not Empty Buffer
     Remaining updates                   :    <1...max>
     Remaining updates (same version)    :    <1...max>
     New firmware valid for TPM          :    Yes
     TPM family after update             :    2.0
     TPM firmware version after update   :    <new_fw_version>

     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: 0 %
     ...
     Completion: 100 %
     TPM Firmware Update completed successfully.

A system restart is required before the TPM can enter operational mode again.
```

7.4.5 Update a TPM2.0 with already set platform policy (using policy file)

To update a TPM2.0 using an alredy set platform policy with a policy file (see 3.1.2.4 or 4.1.2.4), run the following command:

```
TPMFactoryUpd -update tpm20-platformpolicy -polcyfile policy.cfg -firmware
firmware.bin
```

Example output (e.g. for SLB 9672):

```
*************************************************************************
*    Infineon Technologies AG   TPMFactoryUpd   Ver 02.00.xxxx.00     *
*************************************************************************

     TPM update information:
     -----------------------
     TPM family                          :    2.0
     TPM firmware version                :    <current_fw_version>
     TPM firmware valid                  :    Yes
     TPM operation mode                  :    Operational
     TPM platformAuth                    :    Not Empty Buffer
     Remaining updates                   :    <1...max>
     Remaining updates (same version)    :    <1...max>
     New firmware valid for TPM          :    Yes
     TPM family after update             :    2.0
     TPM firmware version after update   :    <new_fw_version>

     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: 0 %
     ...
     Completion: 100 %
     TPM Firmware Update completed successfully.

A system restart is required before the TPM can enter operational mode again.
```

7.4.6 Update a TPM to latest firmware version

This example 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/TPM20_latest.cfg
```

Example output (e.g. for SLB 9672):

```
*********************************************************************
*    Infineon Technologies AG   TPMFactoryUpd   Ver 02.00.xxxx.00    *
*********************************************************************

     TPM update information:
     -----------------------
     TPM family                          :    2.0
     TPM firmware version                :    <current_fw_version>
     TPM firmware valid                  :    Yes
     TPM operation mode                  :    Operational
     TPM platformAuth                    :    Empty Buffer
     Remaining updates                   :    <1...max>
     Remaining updates (same version)    :    <1...max>
     New firmware valid for TPM          :    Yes
     TPM family after update             :    2.0
     TPM firmware version after update   :    <new_fw_version>

     Selected firmware image:
     TPM20_<new_fw_version>_<fw_revision>.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: 0 %
     ...
     Completion: 100 %
     TPM Firmware Update completed successfully.

A system restart is required before the TPM can enter operational mode again.
```

7.4.7 Update a TPM1.2 Using Deferred Physical Presence

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

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

Example output:

```
*************************************************************************
*    Infineon Technologies AG   TPMFactoryUpd   Ver 02.00.xxxx.00     *
*************************************************************************

     TPM update information:
     -----------------------
     TPM family                          :    1.2
     TPM firmware version                :    <current_fw_version>
     TPM firmware valid                  :    Yes
     TPM operation mode                  :    Operational
     TPM enabled                         :    No
     TPM activated                       :    No
     TPM owner set                       :    No
     TPM deferred physical presence      :    No (Settable)
     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 Deferred Physical Presence preparation successful.

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

     Updating the TPM firmware ...
     Completion: 0 %
     ...
     Completion: 100 %
     TPM Firmware Update completed successfully.

A system restart is required before the TPM can enter operational mode again.
```

7.4.8 Update a TPM1.2 by taking TPM Ownership

To update an unowned TPM1.2 by first taking TPM ownership, run the following command:

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

Example output:

```
*********************************************************************
*    Infineon Technologies AG   TPMFactoryUpd   Ver 02.00.xxxx.00    *
*********************************************************************

     TPM update information:
     -----------------------
     TPM family                          :    1.2
     TPM firmware version                :    <current_fw_version>
     TPM firmware valid                  :    Yes
     TPM operation mode                  :    Operational
     TPM enabled                         :    Yes
     TPM activated                       :    Yes
     TPM owner set                       :    No
     TPM deferred physical presence      :    No (Not settable)
     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: 0 %
     ...
     Completion: 100 %
     TPM Firmware Update completed successfully.

A system restart is required before the TPM can enter operational mode again.
```

Optionally you can override the default owner authorization value with the -ownerauth parameter:

```
TPMFactoryUpd -update tpm12-takeownership -ownerauth owner_auth.secret -
firmware firmware.bin
```

7.4.9 Update a TPM1.2 using existing Owner Authorization

To update an owned TPM1.2 you have to know the owner authorization and store it in a file (for example owner_auth.secret). Run the following command:

```
TPMFactoryUpd -update tpm12-ownerauth -ownerauth owner_auth.secret -firmware
firmware.bin
```

Example output:

```
  ************************************************************************
  *    Infineon Technologies AG   TPMFactoryUpd   Ver 02.00.xxxx.00     *
  ************************************************************************

       TPM update information:
       -----------------------
       TPM family                          :    1.2
       TPM firmware version                :    <current_fw_version>
       TPM firmware valid                  :    Yes
       TPM operation mode                  :    Operational
       TPM enabled                         :    Yes
       TPM activated                       :    Yes
       TPM owner set                       :    Yes
       TPM deferred physical presence      :    No (Not settable)
       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 Owner authorization was verified successfully.

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

       Updating the TPM firmware ...
       Completion: 0 %
       ...
       Completion: 100 %
       TPM Firmware Update completed successfully.

A system restart is required before the TPM can enter operational mode again.
```

7.4.10 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
```

Example output:

```
*********************************************************************
*    Infineon Technologies AG   TPMFactoryUpd   Ver 02.00.xxxx.00    *
*********************************************************************

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

Optionally you can override the default owner authorization value with the -ownerauth parameter:

```
TPMFactoryUpd -tpm12-clearownership -ownerauth owner_auth.secret
```

7.4.11 Show Help

To explicitly show the help, run the following command:

```
TPMFactoryUpd -help
```

7.4.12 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.

7.5 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. A detailed error message is shown on the screen and a log entry is written, too. The error codes specific to Infineon TPM Factory Update Tool can be divided in two categories which are listed below.

7.5.1 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 7.1 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 missing or invalid.
0xE029500A	The selected command line option cannot be used with the TPM family or device.
0xE029500B	The selected command line option cannot be used in the current TPM state.
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 or can function properly again.
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 or recover existing firmware with option '-update config-file' because file 'TPMFactoryUpd_RunData.txt' is missing.
0xE029551B	A newer revision of the firmware image is required.
0xE0295522	TPM1.2: The owner authorization is invalid.
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.

Error Code	Error Message
0xE029552A	The TPM1.2 failed the self-test. TPM firmware update is not possible. Restart the system and try again.
0xE029552B	An invalid value was passed in the <ownerauth> command line option.
0xE029552C	An invalid value was passed in the <policyhandle> command line option. Set up policy session and try again.

7.5.2 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.

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.

8 References

[1] "SLB 9645 TPM1.2 Basic Platform Manufacturer Guideline, CONFIDENTIAL, Distribution under NDA only".

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

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

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

[5] "TCG TPM v2.0 Provisioning Guidance," March 15 2017. [Online]. Available: https://trustedcomputinggroup.org/wp-content/uploads/TCG-TPM-v2.0-Provisioning-Guidance-Published-v1r1.pdf.

Revision History

Major changes since revision 1.0

Page or Reference	Description of change
7.4	TPMFactoryUpd displays the number of remaining updates
7.4	TPMFactoryUpd displays when chip is set to factory defaults
4.3, 7.4, 7.5	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
4.1.1, 4.1.2, 4.2.2	Updated pictures
4.1.2	Added Attention note to EmptyBuffer usage
All	Use new document template
All	Added Linux relevant information
7.4	TPMFactoryUpd displays the value of deferred physical presence for TPM1.2 TPMFactoryUpd displays platformAuth state for TPM2.0
7.5.1	Added additional Error Codes
All	Added “-update config-file” option

Major changes since revision 1.5

Page or Reference	Description of change
All	Added information about cross version update Added naming of firmware images

Major changes since revision 1.6

Page or Reference	Description of change
All	Added support for SLB 9615, SLB 9645, SLB 9655 and SLB 9656 devices
7.2	Updated config-file option for new devices

Major changes since revision 1.7

Page or Reference	Description of change
5	Added new multi source image format to naming of firmware images

Major changes within revision 2.0

Page or Reference	Description of change
All	Minor updates
3	Added new chapter for SLB 9672 device
5	Added own chapter for naming of firmware images
7	Updated tool command-line, tool output and configuration file usage

Major changes within revision 2.1

Page or Reference	Description of change

7.1	Fixed description of parameter -setmode

Major changes within revision 2.3

Page or Reference	Description of change
3.1, 4.1, 7.1	Added update type tpm20-platformpolicy with optional parameters policyhandle or policyfile Added section for policy configuration file
7.2	Removed config file parameter description for some older devices

Trademarks
All referenced product or service names and trademarks are the property of their respective owners.

Edition 2024-07-05
Published by
Infineon Technologies AG
81726 Munich, Germany

Do you have a question about this document?
Email:
CSSCustomerService@infineon.com

Document reference
IFX-TPM_FactoryUpd_UM