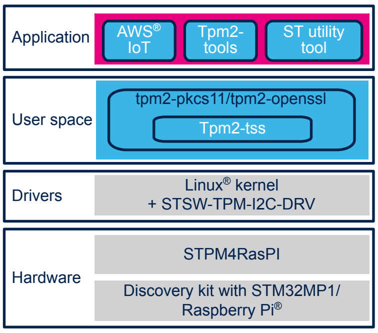
STSW-TPM-I2C-DRV

Data brief

TCG Trusted Platform Module I²C Linux® driver



Features

- Patch for native Linux® kernels:
  - Intended for use with STMicroelectronics TPM devices with an I²C interface (ST33TPHF20I2C, ST33TPHF2XI2C, ST33TPHF2EI2C, ST33GTPMAI2C and ST33GTPMII2C)
  - Implements the Trusted Platform Module (TPM) interface as defined in the *Trusted® Computing Group (TCG) PC Client Platform TPM Profile (PTP) Specification* Level 00, Revision 01.03 v22 or later

Description

The STSW-TPM-I2C-DRV GitHub project provides a TCG-compliant Linux® I²C driver that is packaged as a patch for the native Linux kernel.

This driver is available for the 5.4 Linux driver and has been validated with the following TPM products: ST33TPHF20I2C, ST33TPHF2XI2C, ST33TPHF2EI2C, ST33GTPMAI2C, ST33GTPMII2C.

The STSW-TPM-I2C-DRV driver is compliant with the *TCG PC Client Platform TPM Profile (PTP) Specification* Level 00, Revision 01.03 v22 or later as supported by the STMicroelectronics TPM products. It is also compliant with the *TCG PC Client Device Driver Design Principles for TPM 2.0*.

It supports polling mode with polling intervals optimized for STMicroelectronics TPM products. It does not support interrupt mode.

Product status link
STSW-TPM-I2C-DRV

Product summary	
Order code	TCG- TPM-I2C-DRV
Description	TCG Linux I²C driver
GitHub link	https://github.com/STMicroelectronics/TCG-TPM-I2C-DRV

1 General information

The patch in the STSW-TPM-I2C-DRV software package is provided as an open source.

It has been successfully integrated with the following I^{2}C TPM devices: ST33TPHF20I2C, ST33TPHF2XI2C, ST33TPHF2EI2C, ST33GTPMAI2C, ST33GTPMII2C. These devices are based on an Arm$^{®}$ core.

Note: Arm is a registered trademark of Arm Limited (or its subsidiaries) in the US and/or elsewhere.

1.1 License

STSW-TPM-I2C-DRV is available in GitHub under GPL v2 license.

1.2 Applying the patch

To apply the patch, download the Linux kernel sources, copy the patch into the `linux/drivers/char` directory and run it from the `char` directory with:

```
patch -b -p0 < patchTPMv_5_4_2.patch.
```

The patch is available from the GitHub link: https://github.com/STMicroelectronics/TCG-TPM-I2C-DRV.

1.3 Supported platforms

Refer to the information on the GitHub web page to obtain an up-to-date list of the platform models used for integration tests.

2 User contribution to Git™

This section is given as a checklist that the user should verify before contributing to improving this repository. It includes links to read should the user find that some topics are unclear.

This checklist mainly focuses on the proper use of Git™.

1. Before opening an issue:

   Check that you are in the right repository (for example for TCG-TPM-I2C-DRV, use this link: https://github.com/STMicroelectronics/TCG-TPM-I2C-DRV/issues).

   Check the following points:

   – Make sure that you are using the latest commit (major releases are tagged, but corrections are available as new commits).

   – Make sure that your issue is a question, feedback or suggestion **related to** the software provided in this repository. Otherwise, for any specific TPM support information you can contact STMicroelectronics through the following e-mail:

     TPMsupport@list.st.com.

   – Make sure that your issue has not already been reported and/or fixed on GitHub, or discussed in a previous issue. Refer to the dashboard for the list of issues and pull requests. Do not forget to browse the closed issues.

2. Posting an issue:

   Check the above mentioned points before filing an issue. Then, to file your issue, use one of the two templates (**Bug Report** and **Other Issue**) available in the **Issues** tab of the repository.

Revision history

Table 1. **Document revision history**

Date	Version	Changes
09-Apr-2021	1	Initial release.

IMPORTANT NOTICE – PLEASE READ CAREFULLY

STMicroelectronics NV and its subsidiaries (“ST”) reserve the right to make changes, corrections, enhancements, modifications, and improvements to ST products and/or to this document at any time without notice. Purchasers should obtain the latest relevant information on ST products before placing orders. ST products are sold pursuant to ST’s terms and conditions of sale in place at the time of order acknowledgement.

Purchasers are solely responsible for the choice, selection, and use of ST products and ST assumes no liability for application assistance or the design of Purchasers’ products.

No license, express or implied, to any intellectual property right is granted by ST herein.

Resale of ST products with provisions different from the information set forth herein shall void any warranty granted by ST for such product.

ST and the ST logo are trademarks of ST. For additional information about ST trademarks, please refer to www.st.com/trademarks. All other product or service names are the property of their respective owners.

Information in this document supersedes and replaces information previously supplied in any prior versions of this document.