# Virtual TPM Proxy Driver for Linux Containers

Authors:
Stefan Berger <stefanb@linux.vnet.ibm.com>

This document describes the virtual Trusted Platform Module (vTPM) proxy device driver for Linux containers.

## Introduction

The goal of this work is to provide TPM functionality to each Linux container. This allows programs to interact with a TPM in a container the same way they interact with a TPM on the physical system. Each container gets its own unique, emulated, software TPM.

## Design

To make an emulated software TPM available to each container, the container management stack needs to create a device pair consisting of a client TPM character device `/dev/tpmX` (with X=0,1,2...) and a 'server side' file descriptor. The former is moved into the container by creating a character device with the appropriate major and minor numbers while the file descriptor is passed to the TPM emulator. Software inside the container can then send TPM commands using the character device and the emulator will receive the commands via the file descriptor and use it for sending back responses.

To support this, the virtual TPM proxy driver provides a device `/dev/vtpmx` that is used to create device pairs using an ioctl. The ioctl takes as an input flags for configuring the device. The flags for example indicate whether TPM 1.2 or TPM 2 functionality is supported by the TPM emulator. The result of the ioctl are the file descriptor for the 'server side' as well as the major and minor numbers of the character device that was created. Besides that the number of the TPM character device is returned. If for example `/dev/tpm10` was created, the number (`dev_num`) 10 is returned.

Once the device has been created, the driver will immediately try to talk to the TPM. All commands from the driver can be read from the file descriptor returned by the ioctl. The commands should be responded to immediately.

## UAPI

**System Message: ERROR/3 (`D:\onboarding-resources\sample-onboarding-resources\linux-master\Documentation\security\tpm\[linux-master][Documentation][security][tpm]tpm_vtpm_proxy.rst`, line 47)**

Unknown directive type "kernel-doc".

```
.. kernel-doc:: include/uapi/linux/vtpm_proxy.h
```

**System Message: ERROR/3 (`D:\onboarding-resources\sample-onboarding-resources\linux-master\Documentation\security\tpm\[linux-master][Documentation][security][tpm]tpm_vtpm_proxy.rst`, line 49)**

Unknown directive type "kernel-doc".

```
.. kernel-doc:: drivers/char/tpm/tpm_vtpm_proxy.c
   :functions: vtpmx_ioc_new_dev
```