integrated devices firmware (e.g. the GbE firmware), as well as firmware for the OEM-specific Embedded Controller, and potentially other devices, such as the already discussed (optional) internal disk, and perhaps any discrete networking devices.

The above (read-only) firmware storage should cover also any platform configuration. Typically the BIOS, ME, and potentially other devices would want to use some parts of the flash partitions to store their own configuration (e.g. which devices to boot from, the MAC address, etc).

It should be stressed that all this firmware should be exposed to the platform (e.g. to the host processor or the EC u-controller) using the standard protocols that would normally be used to fetch the firmware. In most cases this is the SPI protocol.

Disk Storage

In addition to playing the role of a firmware storage (in practice: an SPI flash device), the Trusted Stick might also act as a normal mass storage device, seen by the host as e.g. a USB mass storage device, or an SD card.

Here we should further distinguish between two types of storage that is going to be exposed to the platform (the same applies also in the scenario with an internal trusted disk):

1. A read-only non-encrypted storage containing the system code (i.e. the bootloader, the boot partition, and the root filesystem),
2. A writeable (but encrypted) partition for the user files (i.e. the home directory and perhaps some additional system configuration). The key for the encryption could be derived from: 1) the user provided passphrase (provided via keyboard), optionally combined with: 2) a TPM-released secret which can be used, to some extent, to prevent laptop-replacing Evil Maid attacks (which we discuss at the end of this paper in more detail), 3) and also a secret generated by the Trusted Stick and subject to wiping in case the user requested secure deletion of all user-specific data.

It should be noted that it might not be possible to obtain the user passphrase using the standard keyboard during early phase of the platform boot. It is not expected this to be necessary because all the early boot firmware should not be encrypted, but only read-only protected by the Trusted Stick. However, in case