2. It provides the BIOS firmware. Failure to provide a valid BIOS firmware would render the platform un-bootable.

3. It provides the firmware to some of the integrated devices, such as Ethernet network controller, potentially also other devices. Also, it might provide some of the crucial personally identifiable information, such as the MAC address(es) to be used by the networking device(s).

4. Additionally, the flash chip serves as a storage space for various persistent platform configuration settings, for both the BIOS as well as the Intel ME.

The general idea is to remove the SPI flash chip from the motherboard, and route the wiring to one of the external ports, such as either a standard SD or a USB port, or perhaps even to a custom connector[5]. A Trusted Stick (discussed in the next chapter) would be then plugged into this port before the platform boots, and would be delivering all the required firmware requested by the processor, as well as other firmware and, optionally, all the software for the platform.

One problem is that when the system wants to read the ME or the BIOS firmware, none of the devices, not even the DRAM memory is initialized at this stage. This means we cannot use e.g. a USB controller, and consequently a USB "stick" easily to provide the firmware at this stage. What we can do, however, is to reuse some of the pins in a USB port for the purpose of passing the SPI connections to our Trusted Stick. Ideally these could be multiplexed with original USB port connections, so that after the platform boot is complete, the USB port could be used as a fully featured USB port.[6]

In either case, the goal is to relocate the SPI flash element from the motherboard – where it cannot be neither properly protected (e.g. against software-based reflashing attacks, or physical Evil Maid attacks), nor reliably verified by the user. By relocating it to the Trusted Stick, we

1. provide a reliable way to enforce read-only property of the (select) firmware partitions,

2. allow the user to reliably inspect its content, perhaps using some other (more trusted) machine,

[5]While use of a custom connector might increase the cost of manufacturing of a Stateless Laptop, it might have some advantages related to usability (clear indication to the user where to plug the Trusted Stick), and messaging ("This laptop is *supposed* to be implementing the stateless laptop standard").

[6]Without dynamic multiplexing of these extra signals, we would need to downgrade a USB 3.0 port to USB 2.0, as we would likely need to use the 4 "Super Speed" signals to pipe SPI over them.