separate SPI interfaces: one for the host processor, another to the EC uC. Of course, such an approach is far from ideal, as it increases the amount of signals required for the port to which the Trusted Stick is inserted.[3] As mentioned earlier, a temporary solution might be to use a uC with OTP memory for firmware storage.

It's also not yet clear if the Intel ME (which is part of the processor) would be happy when being put into an environment where the SPI flash it gets access to is externally forced to be read-only. Should this be the case, it might be necessary for the Trusted Stick to allow selective write-access for the ME partition accesses. In that case this region should be encrypted by the Trusted Stick, as already discussed earlier. This is to assure that in case the processor wanted to store some user-compromising secrets there, these secrets would not fall into the hands of an adversary. While this solution might seem simple enough, a slight complication might arise from the inability to ask the user for a passphrase (at least using the standard keyboard) upon early platform boot. In that case we would likely need to use a key kept on the Trusted Stick which is not conditioned on user passphrase to protect these partitions. It might be even possible to use auto-generated, discard-able keys for this purpose. Further research is needed.

Host OS implementation considerations

As previously noted the host OS should be engineered so that it was able to boot and operate efficiently from read-only storage. This is generally not a problem today: many Linux distributions support such a mode of operation (LiveUSB). It does however present some challenges for systems which aggressively try to decompose their TCB, such as Qubes OS [16]. Such systems would like to keep all the USB subsystem, drivers, and devices into separate de-privileged domains (VMs). In order to keep such USB-hosting domain(s) truly untrusted, while at the same time use it as a provider (backend) for the system root storage, special additional mechanisms would have to be used [12]. This complication could be avoided, however, when an internal trusted disk was used on the stateless laptop.

[3] And we would like to keep these down to a minimum in order to be able to re-use existing USB or SD ports.