ARM TrustZone tpm

Some arm devices have physical tpm chips installed, while others do not. The arm specification neither requires nor forbids tpm devices.

All arm v8 devices must implement TrustZone as part of its specification. TrustZone does not implement the tpm specification.

However, since it provides a location for secure computation, software can implement tpm protocols safely while running inside the SecureWorld.

In order to implement the tpm protocols, the software implementation needs someplace to store data securely. For example, the tpm needs a place to store private keys securely.

The TrustZone specification does *not* include any form of storage. This means that even with an arm device, there is no guarantee that a software tpm would work. An alternative is if the TrustZone can create encryption keys reliably without in any way leaking them to the Normal World. This not only solves the issue of key creation for the tpm specification, it also enables Secure World software to store information, such as keys, on normal storage, after encrypting it inside Secure World.

Some hardware devices have an ability either to provide secure storage or to generate hardware unique keys exclusively inside Secure World. For those, a combination of:

- OP-TEE
- Software TPM (fTPM) running on OP-TEE in Secure World

can provide full tpm functionality.

References:

- Microsoft's fTPM
- OP-TEE
- OP-TEE OS boot measurement
- Linux kernel support for fTPM