4 March 2015 Study · Transparency

TPMv2 Analysis

The full text is currently only available in the Deutsch version. A translation will follow.

Archived. This content is no longer updated. It remains available for reference.

Source https://technology2.a-sit.at/en/publications/tpmv2-analyse/

The „Trusted Computing“ technology offers interesting concepts and methods to increase the trustworthiness of connected systems. By adding a new component to a computer, it is possible to watch the behaviour of the computer and protect it from unwanted behaviour caused by malicious software. Trusted Computing does not only protect local systems, it also helps to attest the state of a remote system. In 2009 A-SIT evaluated „Trusted Computing“ and its central component the Trusted Platform Module. The study (German only, see download area) engaged on the TPM v1.2, which was enrolled to the mass market.

A-SIT analysed the successor specification TPMv2 and synthesized a TPMv2 emulator from the specifications (results not published).