6 April 2021 Study · Transparency · Web & Cloud

New Trust Models based on Trusted Computing

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 This content is no longer updated.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.

Version 2021-03-26
Source https://technology2.a-sit.at/en/publications/new-trust-models-based-on-trusted-computing/

Traditionally, two basic approaches to implementing trust models exist. On the one hand, there is hierarchical trust (most prominently standardised through PKIX) knowing clearly defined roles, on the other hand, so the concept of a so called web of trust pursues an opposing strategy by foregoing central central instances or predefined hierarchies. The increasing availability of trusted computing (either using Intel's Software Guard Extensions (SGX) or on mobile devices with cryptographic hardware) opens up possibilities to combine both models. In the context of this project, such ways of combining these contrasting trust models were explored. This resulted in developing a hybrid trust model which is rooted in trusted computing to provide a practical way of harnessing the pros of a web of trust while eliminating all the cons.