Recently MicroOS gained some new options in relation with security. The distribution has now integrated Keylime, an open source project for doing remote attestation with TPMS.

If you follow the news about Windows 11, you are aware of what is a TPM. The Trusted Platform Module (TPM) is a cryptoprocessor, described by the Trusted Computing Group (TCG) in a specification that has been standardized in an ISO/IEC document. You can find the TPM already soldered in the mainboard of your computer, but they can also be found as a service in the firmware, or inside your CPU.

This co-processor can be used for many tasks related with security. For example, we can use it to generate symmetric and asymmetric keys, encrypt some memory blocks (not too big, as they are a bit slow), or to as storage for keys that can be used only for us (or applications that have permissions).

Source URL: http://www.tuxmachines.org/node/158321
Links: