On this foundation of identity and trust, we can build …

Safe, mutually signed and acknowledged firmware updates