I found one proposal is “We propose splitting a CA’s private key among multiple parties, and producing signatures using a generic secure multi-party computation protocol that never exposes the actual signing key.”

The proposal is based on MPC.

Is there any possible solution which can be implemented with smart contract?