I am interested in implementing cryptographic primitives on top of MPC. Specifically such that a private key can be generated and used inside of a private computation. (Only the MPC/SGX instance would have access to the key.)

Is this type of functionality already natively available for Enigma? Or should I implement this myself using smart contracts? (And hopefully, if performance allows, be able to execute them using MPC instead of SGX in the future?)