

THE PROBLEM TECHNICALLY



Confidentiality requires only consumer is in control of key material. Or in other words, nobody can access your password or secret key.



Consumers are unable to simultaneously ensure confidentiality and availability of keys.



Cryptographic key-splitting solutions so far are not usable.



Regulation¹ forces European e-money issuers using electronic wallets to enable consumers to always recover their electronic funds (i.e. if devices are lost).

¹ According to ECB

