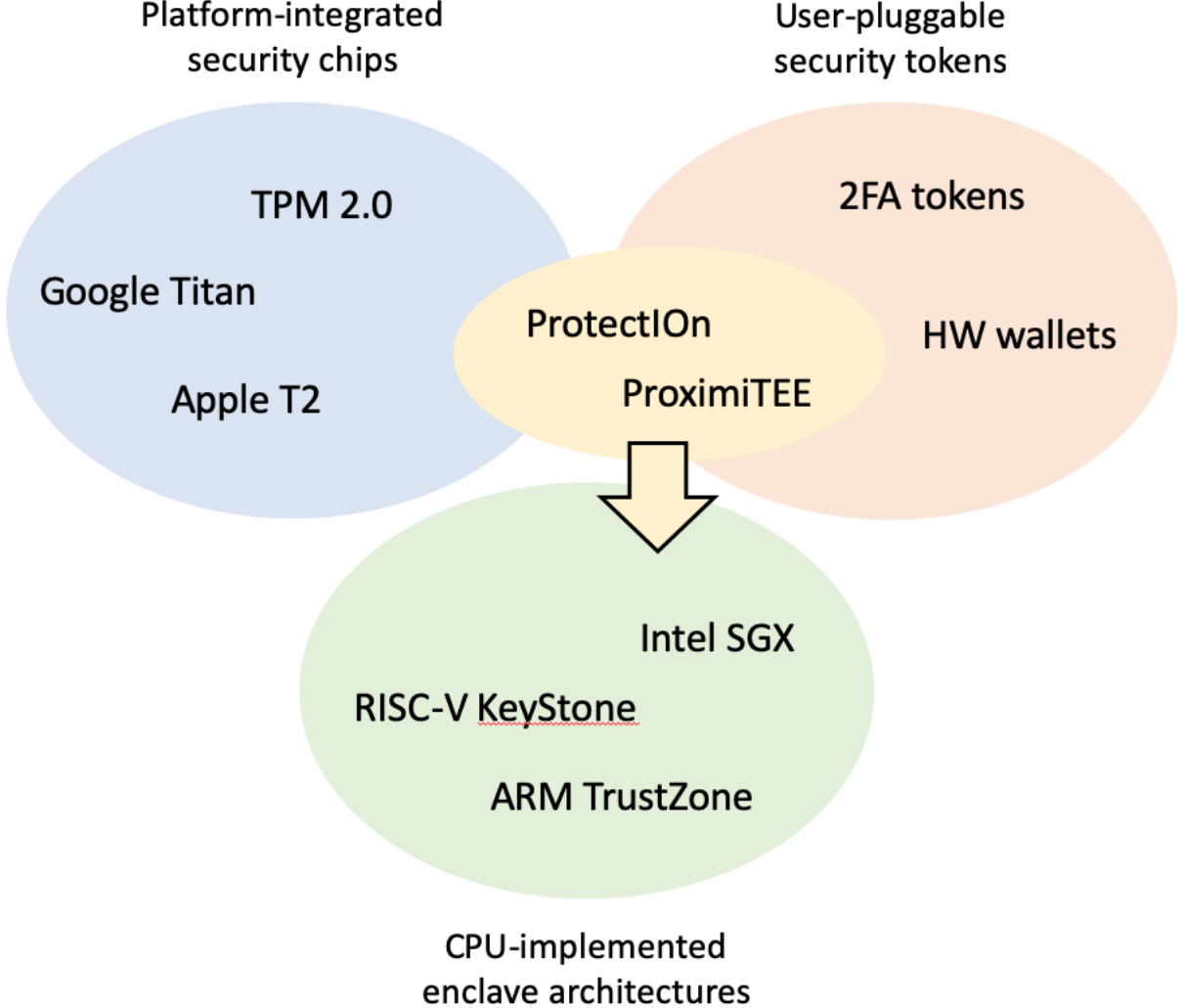
Platform-integrated
security chips
User-pluggable
security tokens
TPM 2.0
Google Titan
Apple T2
2FA tokens
HW wallets
ProtectIOn
ProximiTEE
Intel SGX
RISC-V KeyStone
ARM TrustZone
CPU-implemented
enclave architectures