

1a.Client→PM	: Authentication Request
2a.PM→PAL	: Invoke PAL with "Authentication Block"
2b.PM→PAL	: sealedPassList
3a.Client↔PAL	: Execute Secure Tunnel Protocol
3b.Client	: Store PALpub
3c.Client→PAL	: User ID and Password (master or OTP[n])
4a.PAL	: PassList= TPMUnSeal(sealedPassList,PCR18)
4b.PAL	: validate User ID and Password from PassList
4c.PAL	: If (valid) TPMExtend("1",PCR18) else TPMExtend("0",PCR18)
5a.PAL→PM	: Validation Result (fail or success)
6a.PM	: Execute Attestation Protocol
6b.PM→Client	: If validation = "fail", send error and abort