

1a.PM	: Generate an RSA keypair (PMpriv,PMpub)
1b.PM	: TPMExtend(PMpub,PCR15)
1c.PM	: Validate the hash of PAL
2a.PM→PAL	: Invoke PAL with "Initial Sealing Block"
2b.PM→PAL	: PMPub
3a.PAL	: hash=Hash("0"+Hash(PMPub))
3b.PAL	: validate PMPub by checking hash=PCR15
3c.PAL	: sealedPMPub=TPMSeal(PMPub,PCR18)
4a.PAL→PM	: sealedPMPub
5a.PM	: Store sealedPMPub