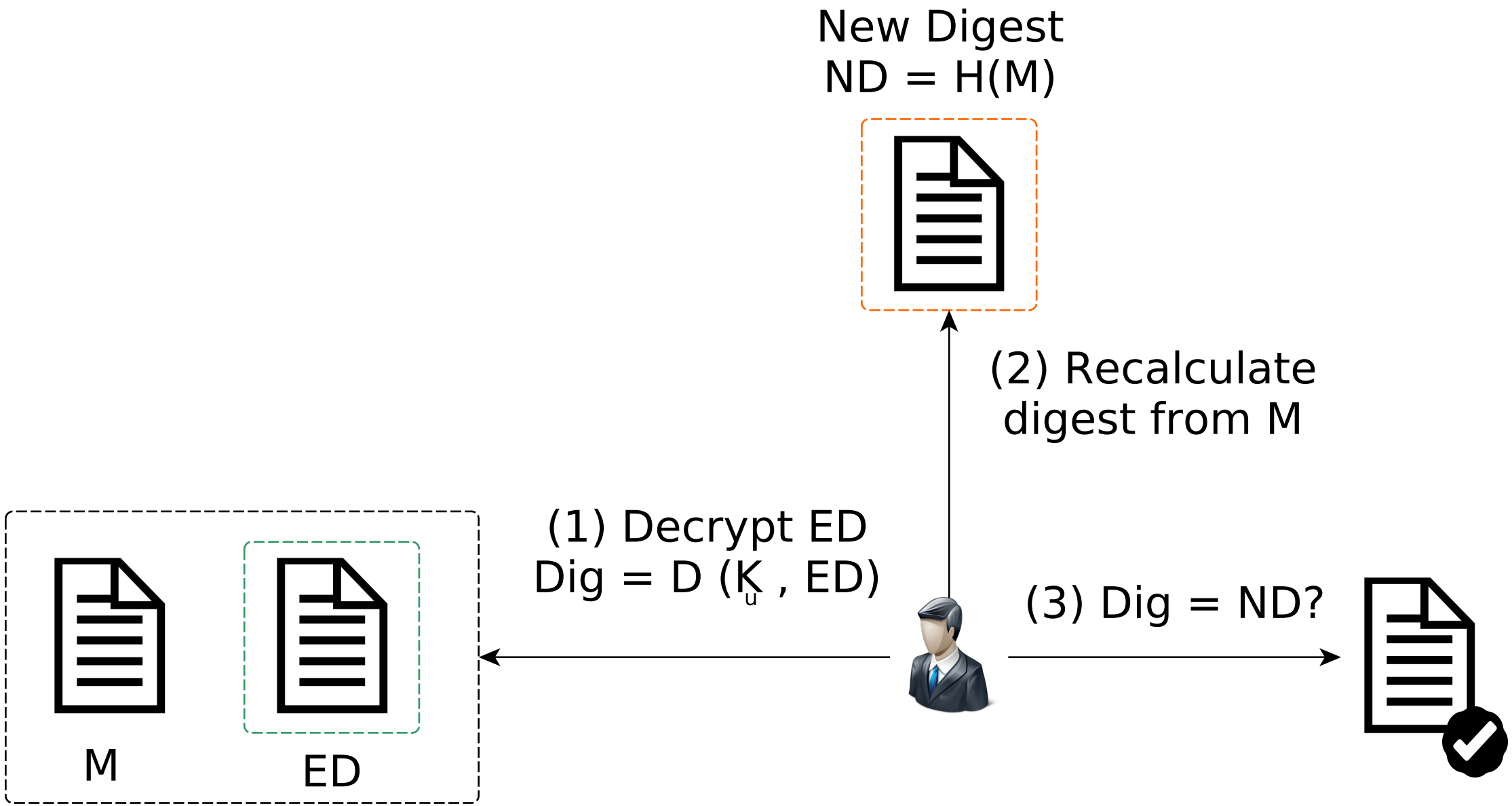
New Digest
ND = H(M)
(2) Recalculate
digest from M
(1) Decrypt ED
Dig = D (K u , ED)
(3) Dig = ND?
M
ED