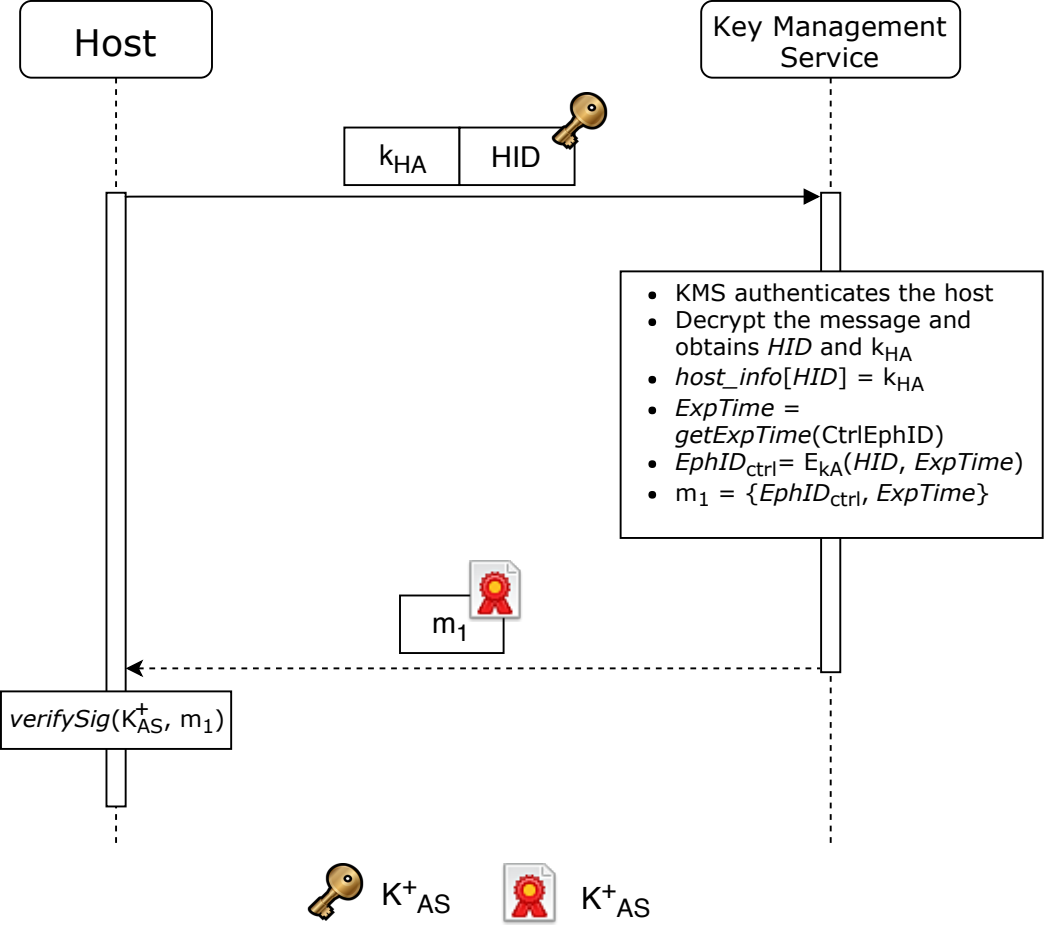
Host
Key Management Service
k_{HA}
HID
KMS authenticates the host
Decrypt the message and obtains *HID* and k_{HA}
host_info[*HID*] = k_{HA}
ExpTime = *getExpTime*(CtrlEphID)
$EphID_{ctrl}$= E_{kA}(*HID*, *ExpTime*)
m_1 = {$EphID_{ctrl}$, *ExpTime*}
m_1
verifySig(K^+_{AS}, m_1)
K^+_{AS}
K^+_{AS}