~M_3 = AES_CMAC(AES_CMAC(AES_CMAC(ZERO, concat(concat(concat(PI,PCap),PS),p256(gen,exp_P_1)),a_1)),p256(a_1,exp_P_1)),prck),concat(rand_prov_2,static_oobdata))

