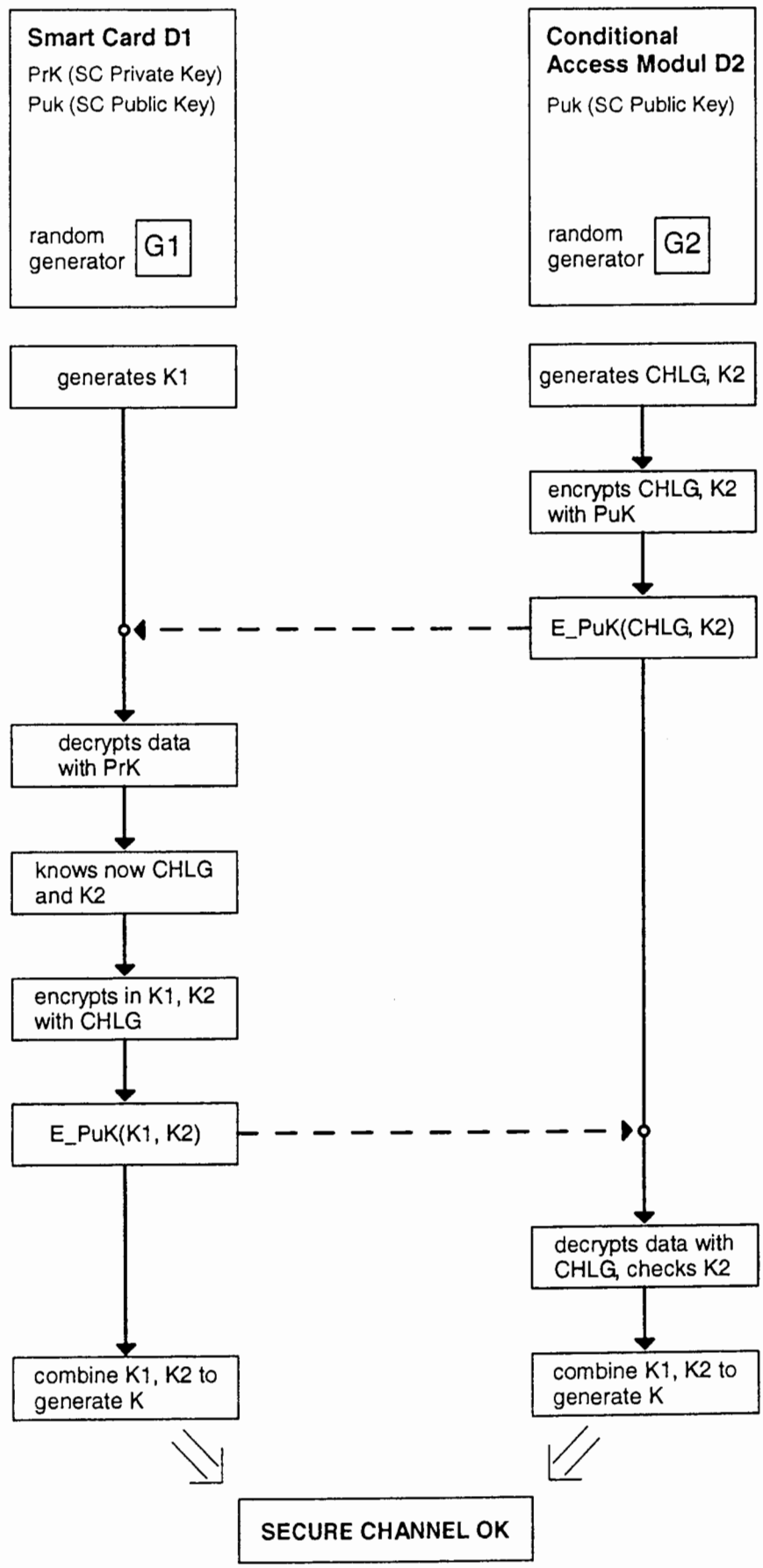

Smart Card D1
PrK (SC Private Key)
Puk (SC Public Key)
random generator
G1
Conditional Access Modul D2
Puk (SC Public Key)
random generator
G2
generates K1
generates CHLG, K2
encrypts CHLG, K2 with PuK
E_PuK(CHLG, K2)
decrypts data with PrK
knows now CHLG and K2
encrypts in K1, K2 with CHLG
E_PuK(K1, K2)
decrypts data with CHLG, checks K2
combine K1, K2 to generate K
combine K1, K2 to generate K
SECURE CHANNEL OK