BLIND TRUST OF CERTIFICATE AUTHORITIES

DESCRIPTION

Blind trust of the signing authorities of the received certificate without further verification of the authorities or the certificate revoking list

ATTACK VECTOR

Self-signed certificate or certificate signed by rogue RA. Attack Codes: a_A0 a_A1 a_S0 a_S5

CONSEQUENCE

Possible leaking out communication information to adversary. Defence Codes: d_D2 d_D5 d_D10 d_D11 d_D13 d_D14 d_E1 d_M1 d_M5 d_M18 d_P0 d_P1 d_P8

v_E4