

Abbreviations
~M_2 = derive_encryption_key(exp(exp(g,derive_prikey_from_sn(serial_number_const)),pri_c),a)
~M_3 = exp(g,pri_c)
~M_4 = pre_app1
~X_1 = (serial_number_const,(~M_2,pre_app1)) = (serial_number_const, (derive_encryption_key(exp(exp(g,pri_c),derive_prikey_from_sn(serial_number_const)),a),pre_app1))
~M_11 = AES_enc(smarthings_const,derive_key(derive_encryption_key(exp(exp(g,pri_c),derive_prikey_from_sn(serial_number_const)),a),bleAuthentication_const),a_2)
~M_12 = open_ch
~X_2 = (AES_enc(smarthings_const,derive_key(~M_2,bleAuthentication_const),~M_9),open_ch) = (AES_enc(smarthings_const,derive_key(derive_encryption_key(exp(exp(g,pri_c),derive_prikey_from_sn(serial_number_const)),a),bleAuthentication_const),n2_2),open_ch)
~M_13 = AES_enc(serial_number_const,derive_key(derive_encryption_key(exp(exp(g,pri_c),derive_prikey_from_sn(serial_number_const)),a),n2_2),n2_2)
~M_14 = open_ch
~M_15 = AES_enc(serial_number_const,derive_key(derive encryption_key(exp(exp(g,pri_c),derive_prikey_from_sn(serial_number_const)),a),n2_2),n2_2)
~M_16 = open_ch
~X_3 = (AES_enc(~M_7,derive_key(~M_2,~M_9),~M_9),open_ch) = (AES_enc(secure_param_4,derive_key(derive_encryption_key(exp(exp(g,pri_c),derive_prikey_from_sn(serial_number_const)),a),n2_2),n2_2),open_ch)
~X_4 = (get_id(derive_key(derive_encryption_key(exp(exp(g,pri_c),derive_prikey_from_sn(serial_number_const)),a),privacy_const),secure_param_4,secure_param_4,secure_param_4),id_s)
~X_5 = (get_id(derive_key(derive_encryption_key(exp(exp(g,pri_c),derive_prikey_from_sn(serial_number_const)),a),privacy_const),secure_param_4,secure_param_4,secure_param_4),id_p)

