Abbreviations
~M_1 = nonce_6
~M_2 = rpid_7
~M_3 = senc(Auth1(username_4,rpid_7,skA_2),wk_2)
~M_4 = dhexp(g,dh_spairRP_2)
~M_5 = sign(RP1(nonce_6,rpid_7,senc(Auth1(username_4, rpid_7,skA_2),wk_2),dhexp(g,dh_spairRP_2)),sskey_RP_3)
~M_6 = dhexp(g,dh_spairRP_2)
~M_7 = sign(RP1(nonce_6,rpid_7,senc(Auth1(username_4, rpid_7,skA_2),wk_2),dhexp(g,dh_spairRP_2)),sskey_RP_3)
~X_1 = (hash(Client1(rpid_7,nonce_6)),HMAC(pinAuth_3, hash(Client1(rpid_7,nonce_6))),RP1(nonce_6,rpid_7, senc(Auth1(username_4,rpid_7,skA_2),wk_2),dhexp(g,dh_spairRP_2)),sign(RP1(nonce_6,rpid_7,senc(Auth1(username_4,rpid_7,skA_2),wk_2),dhexp(g,dh_spairRP_2)), sskey_RP_3))
~X_2 = (Auth4(Auth2(h(rpid_7),aaguid_4,senc(Auth1(username_4, rpid_7,skA_2),wk_2),spk(skA_2)),sign(Auth3(Auth2(h(rpid_7),aaguid_4,senc(Auth1(username_4,rpid_7, skA_2),wk_2),spk(skA_2)),hash(Client1(rpid_7,nonce_6))), skA_2),senc(Auth1(username_4,rpid_7,skA_2),wk_2), RP1(nonce_6,rpid_7,senc(Auth1(username_4,rpid_7, skA_2),wk_2),dhexp(g,dh_spairRP_2)),dhexp(g,dh_spairA_2)), sign(Auth4(Auth2(h(rpid_7),aaguid_4,senc(Auth1(username_4,rpid_7,skA_2),wk_2),spk(skA_2)),sign(Auth3(Auth2(h(rpid_7),aaguid_4,senc(Auth1(username_4, rpid_7,skA_2),wk_2),spk(skA_2)),hash(Client1(rpid_7, nonce_6))),skA_2),senc(Auth1(username_4,rpid_7, skA_2),wk_2),RP1(nonce_6,rpid_7,senc(Auth1(username_4, rpid_7,skA_2),wk_2),dhexp(g,dh_spairRP_2)),dhexp(g,dh_spairA_2)),sskey_RP_3))
~M_8 = h(rpid_7)
~M_9 = aaguid_4
~M_10 = senc(Auth1(username_4,rpid_7,skA_2),wk_2)
~M_11 = spk(skA_2)
~M_12 = sign(Auth3(Auth2(h(rpid_7),aaguid_4,senc(Auth1(username_4,rpid_7,skA_2),wk_2),spk(skA_2)), hash(Client1(rpid_7,nonce_6))),skA_2)
~M_13 = senc(Auth1(username_4,rpid_7,skA_2),wk_2)
~M_14 = nonce_6
~M_15 = rpid_7
~M_16 = senc(Auth1(username_4,rpid_7,skA_2),wk_2)
~M_17 = dhexp(g,dh_spairRP_2)
~M_18 = dhexp(g,dh_spairA_2)
~M_19 = sign(Auth4(Auth2(h(rpid_7),aaguid_4,senc(Auth1(username_4,rpid_7,skA_2),wk_2),spk(skA_2)), sign(Auth3(Auth2(h(rpid_7),aaguid_4,senc(Auth1(username_4,rpid_7,skA_2),wk_2),spk(skA_2)),hash(Client1(rpid_7,nonce_6))),skA_2),senc(Auth1(username_4, rpid_7,skA_2),wk_2),RP1(nonce_6,rpid_7,senc(Auth1(username_4,rpid_7,skA_2),wk_2),dhexp(g,dh_spairRP_2)), dhexp(g,dh_spairA_2)),sskey_RP_3)
~M_20 = rpid_7
~M_21 = nonce_6
~X_3 = (Auth4(Auth2(h(~M_2),~M_9,~M_3,~M_11),~M_12,~M_3, RP1(~M_1,~M_2,~M_3,~M_6),~M_18),~M_19,Client1(~M_2,~M_1)) = (Auth4(Auth2(h(rpid_7),aaguid_4, senc(Auth1(username_4,rpid_7,skA_2),wk_2),spk(skA_2)),sign(Auth3(Auth2(h(rpid_7),aaguid_4,senc(Auth1(username_4,rpid_7,skA_2),wk_2),spk(skA_2)), hash(Client1(rpid_7,nonce_6))),skA_2),senc(Auth1(username_4,rpid_7,skA_2),wk_2),RP1(nonce_6,rpid_7, senc(Auth1(username_4,rpid_7,skA_2),wk_2),dhexp(g,dh_spairRP_2)),dhexp(g,dh_spairA_2)),sign(Auth4(Auth2(h(rpid_7),aaguid_4,senc(Auth1(username_4, rpid_7,skA_2),wk_2),spk(skA_2)),sign(Auth3(Auth2(h(rpid_7),aaguid_4,senc(Auth1(username_4,rpid_7, skA_2),wk_2),spk(skA_2)),hash(Client1(rpid_7,nonce_6))), skA_2),senc(Auth1(username_4,rpid_7,skA_2),wk_2), RP1(nonce_6,rpid_7,senc(Auth1(username_4,rpid_7, skA_2),wk_2),dhexp(g,dh_spairRP_2)),dhexp(g,dh_spairA_2)), sskey_RP_3),Client1(rpid_7,nonce_6))

A trace has been found, assuming the following hypothesis:
The attacker has ~M_6 = dhexp(g,dh_spairRP_2[])
The attacker has ~M_7 = sign(RP1(nonce_6[],rpid_7[], senc(Auth1(username_4[],rpid_7[],skA_2[]),wk_2[]), dhexp(g,dh_spairRP_2[])),sskey_RP_3[])