| Abbreviations |
| --- |
| ~X_1 = (a_4,discoveredParticipant,participant_data(~M_12, ~M_4,~M_15,discoveryRegister)) = (a_4,discoveredParticipant, participant_data(GUIDA_4,Topic_bd_4,QoSA_2,discoveryRegister)) |
| ~M_22 = sign_cert(GUIDA_4,pk(PrivKA_1),SN_CI,SK_CI) |
| ~M_23 = sign_perm(GUIDA_4,DGA_1,PPA_1,SK_Perm) |
| ~M_24 = GUIDA_4 |
| ~M_25 = Topic_bd_4 |
| ~M_26 = QoSA_2 |
| ~M_27 = discoveryRegister |
| ~M_28 = ID_G |
| ~M_29 = DH_RSA |
| ~M_30 = SHA256 |
| ~M_31 = hash(SHA256,Clist2bit(make_C_list(sign_cert( GUIDA_4,pk(PrivKA_1),SN_CI,SK_CI),sign_perm(GUIDA_4, DGA_1,PPA_1,SK_Perm),participant_data(GUIDA_4, Topic_bd_4,QoSA_2,discoveryRegister),make_algo( ID_G,DH_RSA),SHA256))) |
| ~M_32 = ChallengeA_5 |
| ~M_33 = dh_pub(ID_G,dh_k(s_5)) |
| ~X_2 = (make_C_list(~M_22,a_5,a_6,make_algo(ID_G,DH_RSA), SHA256),hash(SHA256,Clist2bit(make_C_list(~M_22, a_5,a_6,make_algo(ID_G,DH_RSA),SHA256))),a_7,a_8) = (make_C_list(sign_cert(GUIDA_4,pk(PrivKA_1), SN_CI,SK_CI),a_5,a_6,make_algo(ID_G,DH_RSA),SHA256), hash(SHA256,Clist2bit(make_C_list(sign_cert(GUIDA_4, pk(PrivKA_1),SN_CI,SK_CI),a_5,a_6,make_algo(ID_G, DH_RSA),SHA256))),a_7,a_8) |
| ~X_3 = (make_C_list(~M_34,~M_35,participant_data(~M_36, ~M_37,~M_38,~M_39),make_algo(~M_40,~M_41),~M_42), ~M_43,~M_44,~M_45,~M_46,~M_47,~M_48,~M_49) = ( make_C_list(sign_cert(GUIDB_4,pk(PrivKB_1),SN_CI, SK_CI),sign_perm(GUIDB_4,DGB_2,PPB_2,SK_Perm), participant_data(GUIDB_4,Topic_bd_4,QosB_3,discoveryRegister), make_algo(ID_G,DH_RSA),SHA256),hash(SHA256,Clist2bit( make_C_list(sign_cert(GUIDB_4,pk(PrivKB_1),SN_CI, SK_CI),sign_perm(GUIDB_4,DGB_2,PPB_2,SK_Perm), participant_data(GUIDB_4,Topic_bd_4,QosB_3,discoveryRegister), make_algo(ID_G,DH_RSA),SHA256))),a_7,ChallengeB_4, dh_pub(ID_G,dh_k(s_6)),hash(SHA256,Clist2bit(make_C_list( sign_cert(GUIDA_4,pk(PrivKA_1),SN_CI,SK_CI),a_5, a_6,make_algo(ID_G,DH_RSA),SHA256))),a_8,sign( PrivKB_1,(hash(SHA256,Clist2bit(make_C_list(sign_cert( GUIDB_4,pk(PrivKB_1),SN_CI,SK_CI),sign_perm(GUIDB_4, DGB_2,PPB_2,SK_Perm),participant_data(GUIDB_4, Topic_bd_4,QosB_3,discoveryRegister),make_algo( ID_G,DH_RSA),SHA256))),ChallengeB_4,dh_pub(ID_G, dh_k(s_6)),a_7,a_8,hash(SHA256,Clist2bit(make_C_list( sign_cert(GUIDA_4,pk(PrivKA_1),SN_CI,SK_CI),a_5, a_6,make_algo(ID_G,DH_RSA),SHA256)))))) |
| ~X_4 = (make_C_list(~M_34,a_9,a_10,make_algo(ID_G,DH_RSA), SHA256),hash(SHA256,Clist2bit(make_C_list(~M_34, a_9,a_10,make_algo(ID_G,DH_RSA),SHA256))),a_11, a_12) = (make_C_list(sign_cert(GUIDB_4,pk(PrivKB_1), SN_CI,SK_CI),a_9,a_10,make_algo(ID_G,DH_RSA),SHA256), hash(SHA256,Clist2bit(make_C_list(sign_cert(GUIDB_4, pk(PrivKB_1),SN_CI,SK_CI),a_9,a_10,make_algo(ID_G, DH_RSA),SHA256))),a_11,a_12) |

A trace has been found.