Abbreviations
~M_1 = senckey((fAKID((fATID(SUPI,K),ID_MNO_5)),ID_AF_5,hmac((user_id,ID_AF_5),K_UE)),KEMkey(Encaps(pk(SK_MNO),rUE_1)))
~M_2 = KEMCipher(Encaps(pk(SK_MNO),rUE_1))
~M_3 = hmac(senckey((fAKID((fATID(SUPI,K),ID_MNO_5)),ID_AF_5,hmac((user_id,ID_AF_5),K_UE)),KEMkey(Encaps(pk(SK_MNO),rUE_1))),KEMkey(Encaps(pk(SK_MNO),rUE_1)))
~M_4 = ID_MNO_5
~M_5 = senckey((fAKID((fATID(SUPI,K),ID_MNO_5)),ID_AF_5,hmac((user_id,ID_AF_5),K_UE)),KEMkey(Encaps(pk(SK_MNO),rUE_2)))
~M_6 = KEMCipher(Encaps(pk(SK_MNO),rUE_2))
~M_7 = hmac(senckey((fAKID((fATID(SUPI,K),ID_MNO_5)),ID_AF_5,hmac((user_id,ID_AF_5),K_UE)),KEMkey(Encaps(pk(SK_MNO),rUE_2))),KEMkey(Encaps(pk(SK_MNO),rUE_2)))
~M_8 = ID_MNO_5
~X_1 = (senckey((fAKID((fATID(SUPI,K),ID_MNO_5)),ID_AF_5,hmac((user_id,ID_AF_5),K_UE)),KEMkey(Encaps(pk(SK_MNO),rUE_2))),KEMCipher(Encaps(pk(SK_MNO),rUE_2)),hmac(senckey((fAKID((fATID(SUPI,K),ID_MNO_5)),ID_AF_5,hmac((user_id,ID_AF_5),K_UE)),KEMkey(Encaps(pk(SK_MNO),rUE_2))),KEMkey(Encaps(pk(SK_MNO),rUE_2))),ID_AF_5)

A trace has been found.

Honest Process

Attacker

{1}new ID_MNO_5

{2}new ID_AF_5

~M = pk(SK_MNO)

!

!

!

Beginning of process AF

{91}insert choosechannel(ID_MNO_5,chMNOAF)

Beginning of process AF

{91}insert choosechannel(ID_MNO_5,chMNOAF)

Beginning of process MNO

{54}event MNOhasKAKMA(fKAKMA(SUPI,K))

{56}event MNOhasAKID(fAKID((fATID(SUPI,K),ID_MNO_5)))

{57}event indatabase(fAKID((fATID(SUPI,K),ID_MNO_5)),SUPI,fKAKMA(SUPI,K))

{58}insert database(fAKID((fATID(SUPI,K),ID_MNO_5)),SUPI,fKAKMA(SUPI,K))

Beginning of process UE

{14}event UEhasKAKMA(fKAKMA(SUPI,K))

{17}event UEhasAKID(fAKID((fATID(SUPI,K),ID_MNO_5)))

{19}event UEhasKAF(fKAF(ID_AF_5,fKAKMA(SUPI,K)))

{22}event UEhasT(hmac((user_id,ID_AF_5),K_UE))

{24}new rUE_2

{26}event UEhasKsh(KEMkey(Encaps(pk(SK_MNO),rUE_2)))

{29}event UEhasN(senckey((fAKID((fATID(SUPI,K),ID_MNO_5)),ID_AF_5,hmac((user_id,ID_AF_5),K_UE)),KEMkey(Encaps(pk(SK_MNO),rUE_2))))

{32}event UEhasKpAF(KDF2(KEMkey(Encaps(pk(SK_MNO),rUE_2)),fKAF(ID_AF_5,fKAKMA(SUPI,K))))

{33}event UEsendReqAF(senckey((fAKID((fATID(SUPI,K),ID_MNO_5)),ID_AF_5,hmac((user_id,ID_AF_5),K_UE)),KEMkey(Encaps(pk(SK_MNO),rUE_2))),hmac(senckey((fAKID((fATID(SUPI,K),ID_MNO_5)),ID_AF_5,hmac((user_id,ID_AF_5),K_UE)),KEMkey(Encaps(pk(SK_MNO),rUE_2))),KEMkey(Encaps(pk(SK_MNO),rUE_2))),ID_MNO_5)

{34}event UEbegin(senckey((fAKID((fATID(SUPI,K),ID_MNO_5)),ID_AF_5,hmac((user_id,ID_AF_5),K_UE)),KEMkey(Encaps(pk(SK_MNO),rUE_2))))

Beginning of process UE

{14}event UEhasKAKMA(fKAKMA(SUPI,K))

{17}event UEhasAKID(fAKID((fATID(SUPI,K),ID_MNO_5)))

{19}event UEhasKAF(fKAF(ID_AF_5,fKAKMA(SUPI,K)))

{22}event UEhasT(hmac((user_id,ID_AF_5),K_UE))

{24}new rUE_1

{26}event UEhasKsh(KEMkey(Encaps(pk(SK_MNO),rUE_1)))

{29}event UEhasN(senckey((fAKID((fATID(SUPI,K),ID_MNO_5)),ID_AF_5,hmac((user_id,ID_AF_5),K_UE)),KEMkey(Encaps(pk(SK_MNO),rUE_1))))

{32}event UEhasKpAF(KDF2(KEMkey(Encaps(pk(SK_MNO),rUE_1)),fKAF(ID_AF_5,fKAKMA(SUPI,K))))

{33}event UEsendReqAF(senckey((fAKID((fATID(SUPI,K),ID_MNO_5)),ID_AF_5,hmac((user_id,ID_AF_5),K_UE)),KEMkey(Encaps(pk(SK_MNO),rUE_1))),hmac(senckey((fAKID((fATID(SUPI,K),ID_MNO_5)),ID_AF_5,hmac((user_id,ID_AF_5),K_UE)),KEMkey(Encaps(pk(SK_MNO),rUE_1))),KEMkey(Encaps(pk(SK_MNO),rUE_1))),ID_MNO_5)

{34}event UEbegin(senckey((fAKID((fATID(SUPI,K),ID_MNO_5)),ID_AF_5,hmac((user_id,ID_AF_5),K_UE)),KEMkey(Encaps(pk(SK_MNO),rUE_1))))

Beginning of process MNO

{54}event MNOhasKAKMA(fKAKMA(SUPI,K))

{56}event MNOhasAKID(fAKID((fATID(SUPI,K),ID_MNO_5)))

{57}event indatabase(fAKID((fATID(SUPI,K),ID_MNO_5)),SUPI,fKAKMA(SUPI,K))

{58}insert database(fAKID((fATID(SUPI,K),ID_MNO_5)),SUPI,fKAKMA(SUPI,K))

(~M_1,~M_2,~M_3,~M_4)

(~M_5,~M_6,~M_7,~M_8)

(~M_5,~M_6,~M_7,~M_4)

{93}event AFbegin(senckey((fAKID((fATID(SUPI,K),ID_MNO_5)),ID_AF_5,hmac((user_id,ID_AF_5),K_UE)),KEMkey(Encaps(pk(SK_MNO),rUE_2))))

{94}event AFrecReqUE(senckey((fAKID((fATID(SUPI,K),ID_MNO_5)),ID_AF_5,hmac((user_id,ID_AF_5),K_UE)),KEMkey(Encaps(pk(SK_MNO),rUE_2))),hmac(senckey((fAKID((fATID(SUPI,K),ID_MNO_5)),ID_AF_5,hmac((user_id,ID_AF_5),K_UE)),KEMkey(Encaps(pk(SK_MNO),rUE_2))),KEMkey(Encaps(pk(SK_MNO),rUE_2))),ID_MNO_5)

{95}event AFhasN(senckey((fAKID((fATID(SUPI,K),ID_MNO_5)),ID_AF_5,hmac((user_id,ID_AF_5),K_UE)),KEMkey(Encaps(pk(SK_MNO),rUE_2))))

{108}get choosechannel(ID_MNO_5,chMNOAF)

{96}event AFsendReqMNO(senckey((fAKID((fATID(SUPI,K),ID_MNO_5)),ID_AF_5,hmac((user_id,ID_AF_5),K_UE)),KEMkey(Encaps(pk(SK_MNO),rUE_2))),hmac(senckey((fAKID((fATID(SUPI,K),ID_MNO_5)),ID_AF_5,hmac((user_id,ID_AF_5),K_UE)),KEMkey(Encaps(pk(SK_MNO),rUE_2))),KEMkey(Encaps(pk(SK_MNO),rUE_2))),ID_AF_5)

~X_1

{60}event MNObegin(senckey((fAKID((fATID(SUPI,K),ID_MNO_5)),ID_AF_5,hmac((user_id,ID_AF_5),K_UE)),KEMkey(Encaps(pk(SK_MNO),rUE_2))))

{61}event MNOrecReqAF(senckey((fAKID((fATID(SUPI,K),ID_MNO_5)),ID_AF_5,hmac((user_id,ID_AF_5),K_UE)),KEMkey(Encaps(pk(SK_MNO),rUE_2))),hmac(senckey((fAKID((fATID(SUPI,K),ID_MNO_5)),ID_AF_5,hmac((user_id,ID_AF_5),K_UE)),KEMkey(Encaps(pk(SK_MNO),rUE_2))),KEMkey(Encaps(pk(SK_MNO),rUE_2))),ID_AF_5)

{62}event MNOhasN(senckey((fAKID((fATID(SUPI,K),ID_MNO_5)),ID_AF_5,hmac((user_id,ID_AF_5),K_UE)),KEMkey(Encaps(pk(SK_MNO),rUE_2))))

{64}event MNOhasKshMNO(DecapsKey(SK_MNO,KEMCipher(Encaps(pk(SK_MNO),rUE_2))))

{67}event trMAC(hmac(senckey((fAKID((fATID(SUPI,K),ID_MNO_5)),ID_AF_5,hmac((user_id,ID_AF_5),K_UE)),KEMkey(Encaps(pk(SK_MNO),rUE_2))),DecapsKey(SK_MNO,KEMCipher(Encaps(pk(SK_MNO),rUE_2)))))

{69}event MNOgetAKID(fAKID((fATID(SUPI,K),ID_MNO_5)))

{70}event MNOgetIDAF(ID_AF_5)

{71}event MNOgetT(hmac((user_id,ID_AF_5),K_UE))

{73}event trIDAF(ID_AF_5)

{87}get database(fAKID((fATID(SUPI,K),ID_MNO_5)),SUPI,fKAKMA(SUPI,K))

{75}event yesKAKMA(fKAKMA(SUPI,K))

{77}event MNOhasKAF(fKAF(ID_AF_5,fKAKMA(SUPI,K)))

{80}event MNOhasKpAF(KDF2(DecapsKey(SK_MNO,KEMCipher(Encaps(pk(SK_MNO),rUE_2))),fKAF(ID_AF_5,fKAKMA(SUPI,K))))

{82}event MNOhasHID(hmac((hmac((user_id,ID_AF_5),K_UE),SUPI,ID_AF_5),K_MNO))

{83}event MNOsendResAF(hmac((hmac((user_id,ID_AF_5),K_UE),SUPI,ID_AF_5),K_MNO),fexp(fKAF(ID_AF_5,fKAKMA(SUPI,K))),KDF2(DecapsKey(SK_MNO,KEMCipher(Encaps(pk(SK_MNO),rUE_2))),fKAF(ID_AF_5,fKAKMA(SUPI,K))))

{84}event MNOendN(senckey((fAKID((fATID(SUPI,K),ID_MNO_5)),ID_AF_5,hmac((user_id,ID_AF_5),K_UE)),KEMkey(Encaps(pk(SK_MNO),rUE_2))))

{85}event MNOendKpAF(fKAF(ID_AF_5,fKAKMA(SUPI,K)))