3GPP TSG SA WG3 Security — S3#33 **S3-040256**
10 - 14 May 2004
Beijing, China

Title: **Proposal about the efficient mechanism for the setup of UE-initiated tunnels (Scenario 3) in WLAN interworking**

Source: **ETRI**

Document for: **Discussion and proposal**

Work Item: **WLAN interworking**

1. Introduction

3GPP TS 33.234 v1.0 describes a mechanism for the set-up of UE-initiated tunnels in Scenario 3. In this mechanism, IKEv2 is used to allow IPsec SA establishment between the WLAN UE and the PDGW. UE requires the public key operations in the process of IKEv2 and needs the exchange of 6 times messges to perform EAP-AKA within IKEv2. So, this mechanism imposes heavy burdens on the UE and the PDGW for authentication and key agreement.

2. Discussion

2.1 Outline of our proposal

We propose more efficient authentication mechanism than that of TS 33.234 v1.0 using a secret key distributed in the process of authentication and key agreement between the UE and the 3GPP AAA server. For scenario 3, the access to External IP Networks should, as far as possible, be technically independent of WLAN Access Authentication and Authorisation. However, the access to External IP Networks through 3GPP-WLAN interworking systems shall be possible after WLAN Access Authentication/Authorisation has been completed first. So, we propose the mechanism that a secret key is pre-distributed during WLAN Access Authentication/Authorisation between UE and 3GPP AAA server and then it is used for the set-up of UE-initiated tunnels in Scenario 3.

2.2 Detail of our proposal

It is required that all long-term security credentials used for subscriber and network authentication shall be stored on UICC or SIM card. We consider only the case of UICC in this contribution(similarly to the case of SIM card).

First, we modify the USIM-based WLAN Access Authentication and Key agreement mechanism which is described in 3GPP TS 33.234 v1.0 Section 6.1.1.1. In the figure 1, the parts denoted as italic and red letters, are included additionally.

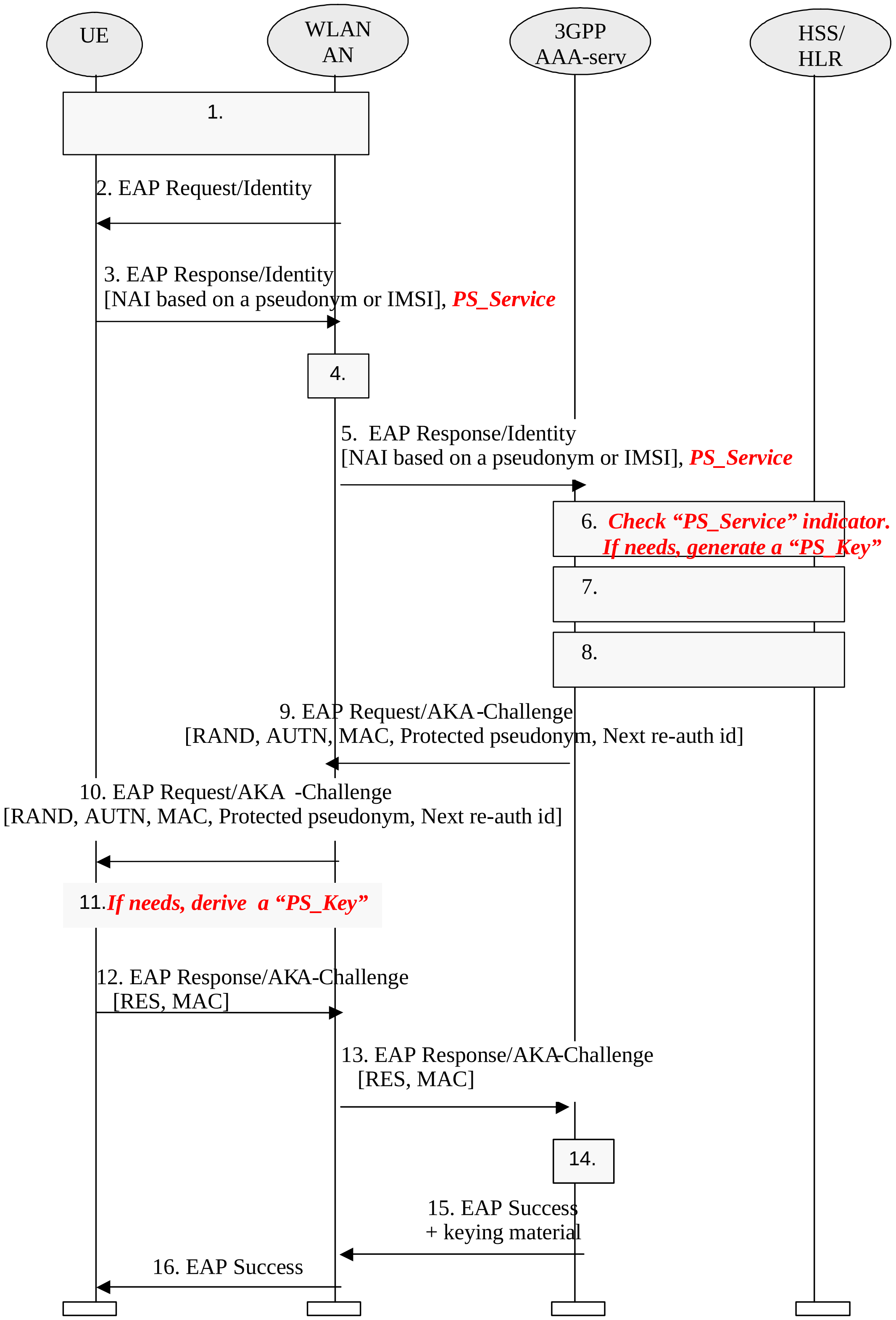
UE
WLAN AN
3GPP AAA-serv
HSS/ HLR
1.
2. EAP Request/Identity
3. EAP Response/Identity
[NAI based on a pseudonym or IMSI], PS_Service
4.
5. EAP Response/Identity
[NAI based on a pseudonym or IMSI], PS_Service
6. Check "PS_Service" indicator.
If needs, generate a "PS_Key"
7.
8.
9. EAP Request/AKA-Challenge
[RAND, AUTN, MAC, Protected pseudonym, Next re-auth id]
10. EAP Request/AKA -Challenge
[RAND, AUTN, MAC, Protected pseudonym, Next re-auth id]
11.If needs, derive a "PS_Key"
12. EAP Response/AKA-Challenge
[RES, MAC]
13. EAP Response/AKA-Challenge
[RES, MAC]
14.
15. EAP Success
+ keying material
16. EAP Success

Figure 1: Authentication based on EAP AKA scheme
[*Figure 4 in 3GPP TS 33.234 v1.0 Section 6.1.1.1*]

In the step 3 of the figure 1, a "PS_Service" parameter indicates that the UE wants to access 3GPP PS Domain based services. In the step 6, 3GPP AAA server checks the "PS_Service" indicator. If the UE want to access 3GPP PS domain based services, a "PS_Key" is generated additionally in the HSS/HLR and UE. HSS/HLR creates "PS_Key" by using 3GPP MILENAGE algorithm like IK and CK generation, and "PS_Key" will be used to setup UE-initiated tunnels in Scenario 3. In the step 11, the WLAN UE also can derive the "PS_Key" by the same method.

After completing the authentication and key agreement between the UE and 3GPP AAA server, the WLAN UE can access the PDGW which provides 3GPP PS Domain based services. To do this, 3GPP TS 33.234 v1.0 is considering to use IKEv2 to setup secure tunnels between the UE and the PDGW. In the process IKEv2, public key cryptography is necessary and it is burden on the UE and the PDGW. However, we propose the efficient method which does not use public key cryptography. It is described as follows.

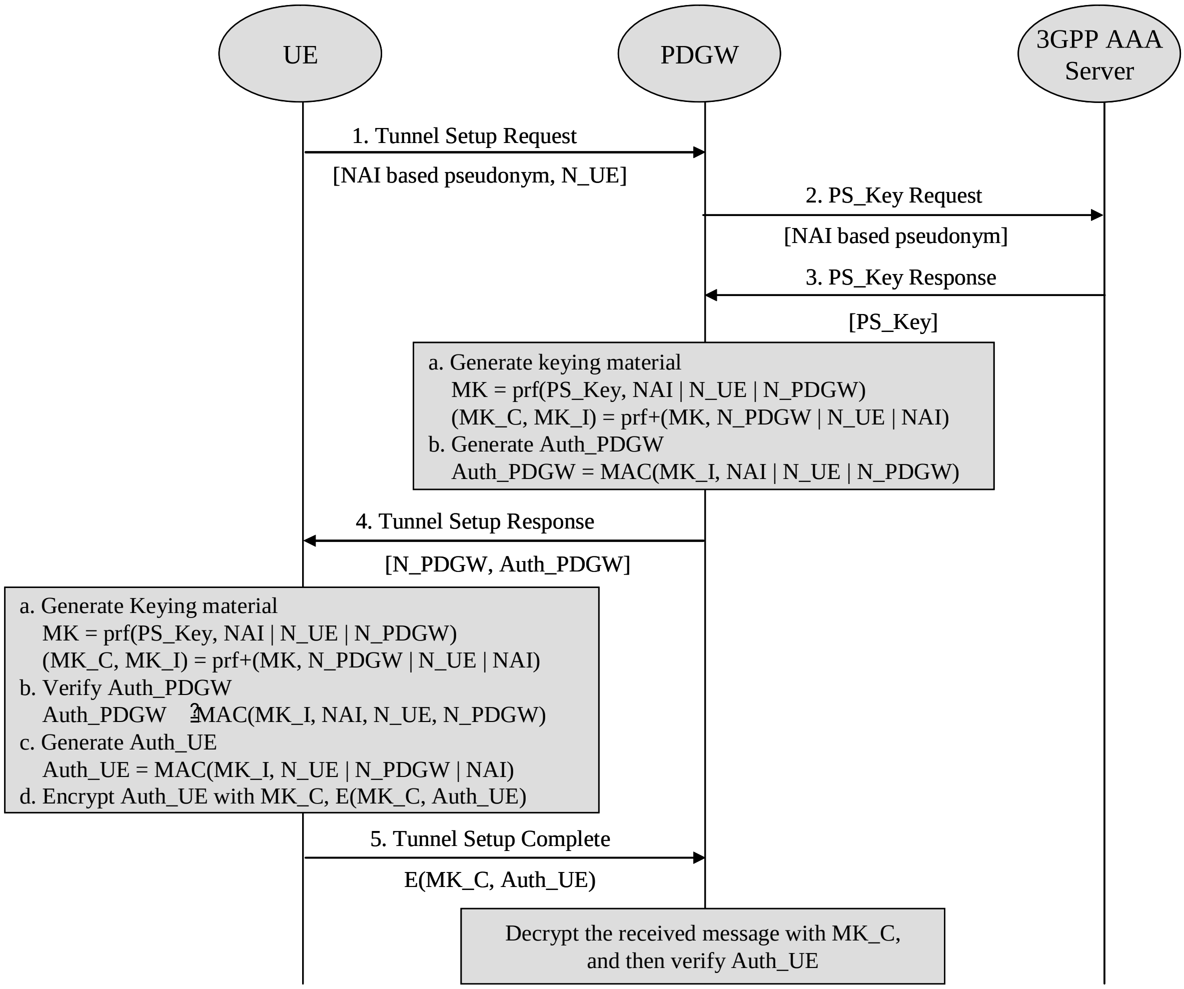
UE
PDGW
3GPP AAA Server
1. Tunnel Setup Request
[NAI based pseudonym, N_UE]
2. PS_Key Request
[NAI based pseudonym]
3. PS_Key Response
[PS_Key]
a. Generate keying material
MK = prf(PS_Key, NAI | N_UE | N_PDGW)
(MK_C, MK_I) = prf+(MK, N_PDGW | N_UE | NAI)
b. Generate Auth_PDGW
Auth_PDGW = MAC(MK_I, NAI | N_UE | N_PDGW)
4. Tunnel Setup Response
[N_PDGW, Auth_PDGW]
a. Generate Keying material
MK = prf(PS_Key, NAI | N_UE | N_PDGW)
(MK_C, MK_I) = prf+(MK, N_PDGW | N_UE | NAI)
b. Verify Auth_PDGW
Auth_PDGW ≟MAC(MK_I, NAI, N_UE, N_PDGW)
c. Generate Auth_UE
Auth_UE = MAC(MK_I, N_UE | N_PDGW | NAI)
d. Encrypt Auth_UE with MK_C, E(MK_C, Auth_UE)
5. Tunnel Setup Complete
E(MK_C, Auth_UE)
Decrypt the received message with MK_C, and then verify Auth_UE

Figure 2. proposed scheme: efficient mechanism for the set-up of UE-initiated tunnels

1. The UE sends "*Tunnel Setup Request*" message. This message includes the pseudonym based NAI which was assigned in the process of the authentication and key agreement between the UE and 3GPP AAA server, and the nonce N_UE generated randomly by the UE.
2. The PDGW routes "*PS_Key Request*" message towards the 3GPP AAA Server indicated on the realm part of the NAI.
3. The 3GPP AAA server sends the subscriber's PS_Key created in the process of the authentication and key agreement between the UE and 3GPP AAA server to the PDGW.
4. The PDGW generates the session master key MK and then derives encryption key MK_C and integrity key MK_I as the following;

    MK = prf(PS_Key, NAI | N_UE | N_PDGW)

    (MK_C, MK_I) = prf+(PS_Key, N_PDGW | N_UE | NAI)

    where N_PDGW is a randomly generated nonce by the PDGW, prf and prf+ are cryptographically secure pseudorandom functions.

    The PDGW computes authenticator Auth_PDGW using MK_I and sends "*Tunnel Setup Response*" message to the UE. This message includes N_PDGW and Auth_PDGW.

    Auth_PDGW = MAC(MK_I, NAI | N_UE | N_PDGW)

5. The UE generates the session master key MK and derives encryption key MK_C and integrity key MK_I using the same method as the PDGW.
   MK = prf(PS_Key, NAI | N_UE | N_PDGW)
   (MK_C, MK_I) = prf+(PS_Key, N_PDGW | N_UE | NAI)
   The UE verifies the received authenticator Auth_PDGW. If Auth_PDGW is correct, the UE computes authenticator Auth_UE using MK_I and sends "*Tunnel Setup Complete*" message to PDGW, which includes encrypted authenticator, E(MK_C, Auth_UE).
6. The PDGW decrypts the received message and then verifies the authenticator Auth_UE. If it succeeds, the PDGW allows the UE to access the service.

3. Conclusion

Our method minimally modifies EAP AKA based authentication mechanism which is described in 3GPP TS 33.234 v1.0. It includes the parameter "PS_Service" additionally in the step 3 of the figure 1, and the generation of PS_Key in the step 6 and the step 11.

For the setup of UE-initiated tunnels, 3GPP TS 33.234 v1.0 is considering IKEv2 to establish a SA. IKEv2 requires modular exponentiation operations to perform Diffie-Hellman key exchange, and public key signature based authentication. However, our proposed scheme is based on only the symmetric key. Therefore, it can avoid modular exponentiation and public key signature which needs a large amount of computation.

As well, our method provides the mutual authentication between the UE and the PDGW. UE authenticates the PDGW by verifying the authenticator Auth_PDG in the step 4 and the PDGW authenticates the UE by checking Auth_UE in the step 5. It guarantees that generated keying materials are unique by nonces N_UE and N_PDGW and cryptographic properties of the prf. Also, the proposed scheme provides the user privacy by sending the pseudonym based NAI in the step 1.