3GPP TSG SA WG3 (Security) Meeting #88Bis **S3-172482**
09 – 13 October, 2017, Singapore

revision of S3-17xabc

Source: **Ericsson**
Title: **Discussion on protection of Network Steering Information**
Document for: **Approval**
Agenda Item: **4.2.15 Others**

1 Decision/action requested

SA3 received an LS from SA2 in S3-171733/S2-175286 requesting SA3 to consider the requirements in the LS for finding a security solution which securs the Network Steering Information from the HPLMN to the UE.

2 References

[1] S3-171733/S2-175286: LS on PLMN and RAT selection policies for roaming

[2] S3-172034: Securing the Network Steering Information (discussion paper from Samsung in SA3#88)

[3] S3-17xxxx/S1-173478: LS on PLMN and RAT selection policies for roaming

[4] S3-17xxxx/C1-173751: Reply LS to LS on PLMN and RAT selection policies for roaming (S2-175286/C1-172866)

3 Rationale

3.1 S3-171733/S2-175286: LS on PLMN and RAT selection policies for roaming

An LS from SA2 was received in SA3 #88 in [1]. The LS from SA2 in [1] states that there is a need to define a standardized way to allow a given HPLMN to provide its roaming UEs with information about preferred networks and RAT depending on the UE current location.

SA2 did submit for consideration the following requirements in [1]:

- a control plane solution is used from the HPLMN to the UE.

- VPLMN is able to relay this information to the UE.

- VPLMN shall not be able to alter the information sent by the HPLMN; i.e. UE needs to be able to check the integrity of the information provided to it.

- UE shall be able to detect if VPLMN alter or remove those information and act accordingly.

SA1 replied in S1-173478 [3] with references to corresponding service requirements in TS 22.261 (subclauses 5.1.2.1 and 6.19), and TS 22.011 (subclause 3.2.2.8). SA1 requiremements seem to stress that the HPLMN needs to be able to steer or redirect the UE for a specific VPLMN **at any time**.

CT1 indicated in C1-173751 that CT1 is responsible for the stage 2 specification (TS 23.122), and asks SA3 to investigate end-to-end security solution based on requirements in [1] before CT1 specifies any solution to the requirements.

3.2 S3-172034: Securing the Network Steering Information

In addition another paper in [2] was submitted to SA3 #88 on this topic.

DOCKET ALARM Find authenticated court documents without watermarks at docketalarm.com.

Two different alternatives were discussed in [2]. The two potential security credentials to be considered to secure the information from the AUSF (in the HPLMN) to the UE were:

1. Using HN asymmetric key
2. Using an anchor key resulted from primary authentication.

In the conclusion in [2], the second alternative - Using an anchor key resulted from primary authentication – was preferred.

As all operators may not support a HN asymmetric key, using an anchor key resulted from primary authentication, seems like the most promising solution.

4 Detailed proposal

The following solution is using a key (i.e. configuration key) derived from Kausf resulted from primary authentication to secure the Network Steering Information (preferred PLMN and RAT list) from the HPLMN to the UE. The AUSF in HPLMN calculates a message authentication code over the Network Steering Information using this configuration key. In this proposal, we don't consider encryption even though we acknowledge that it may be required. Confidentiality protection requirements should be clarified.

Some additional potential parameters to consider as well could be:

- Configuration key identifier:
    - This identifier could tie the configuration key to the Kausf from which is has been derived. It could for example be the RAND;
- Integrity protection algorithm identifier:
    - If the integrity algorithm is not identified separately, it could be the well-known KDF function typically used in 3GPP networks, i.e. HMAC-SHA-256 (cf. 3GPP TS 33.401 Annex A, and TGPP TS 33.220 Annex B);
- Counter:
    - If the same configuration key needs to be used to calculate more than one MAC, then an additional counter is preferred as a parameter for detecting replay protection in the UE.

Figure 4-1 demonstrates an example of the UE Registration procedure when the AUSF in home network performs the integrity protection of the Network Steering Information and includes the security protected Network Steering Information over N12 interface to the AMF/SEAF in VPLMN. The AMF/SEAF sends the protected Network Steering Information to the UE in a NAS message (e.g. Registration Accept message). Note that the example is an optimization, and the HPLMN needs to be able to send the Network Steering Information **at any time** to the UE, i.e. not only during Registration procedure.

DOCKET ALARM
Find authenticated court documents without watermarks at docketalarm.com.

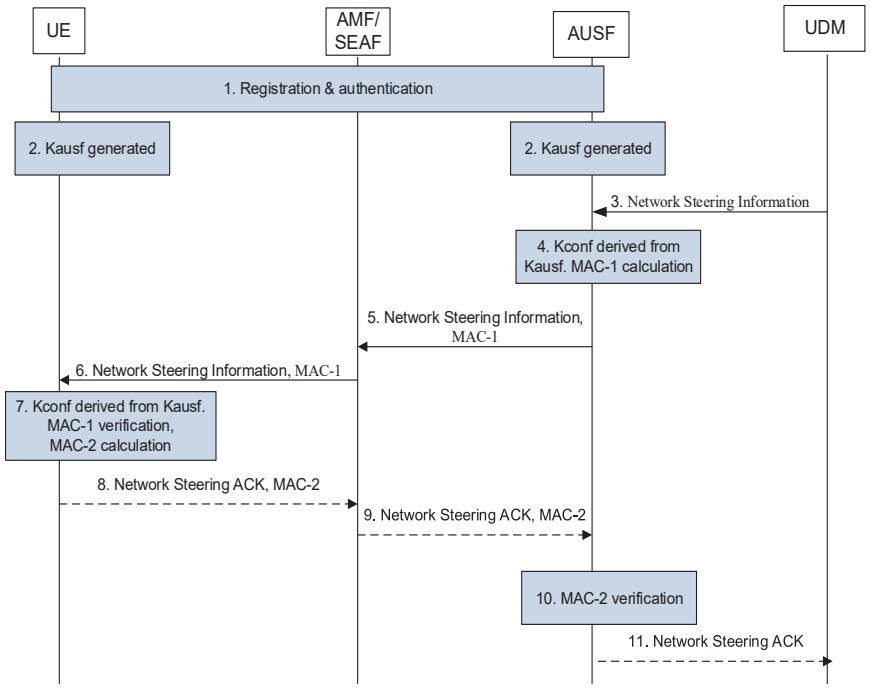

Figure 4-1: Signalling flow showing provisioning of the Network Steering Information from home PLMN to UE

1. The UE registers to the VPLMN, and is authenticated by AUSF.

2. UE and AUSF generate Kausf.

3. A node in the HPLMN (e.g. UDM) sends the Network Steering Information to AUSF. This example assumes that AUSF protects the Network Steering Information, however, it could be some other node, e.g. Policy Control Function.

4. AUSF derives the configuration key (Kconf) from the home network root key (Kausf), and calculates the Message Authentication Code (MAC-1) over Network Steering Information.

5. AUSF forwards the protected Network Steering Information to AMF/SEAF.

6.AMF/SEAF forwards the protected Network Steering Information to the UE. This message could be confidentiality protected over the air with NAS security. Depending on the final architecture, the Network Steering Information could be piggybacked e.g. in Registration Accept message.

7.The UE derives the configuration key (Kconf) from the home network root key (Kausf), and verifies the MAC-1. Depending on the final protocol design, UE may send an acknowledgement message ("Network Steering ACK") to the HPLMN, and protect that information with the MAC-2.

8. The UE sends the protected ACK message to the AMF/SEAF.

9.The AMF/SEAF forwards the protected ACK to the AUSF.

10. AUSF verifies the MAC-2 in the protected Network Steering ACK message.

11. AUSF forwards the ACK to the original source of the Network Steering Information.

Figure 4-2 demonstrates the case when a node other than AUSF (e.g. the Policy Control Function, PCF) is in charge of delivering the Network Steering Information.

DOCKET ALARM
Find authenticated court documents without watermarks at docketalarm.com.

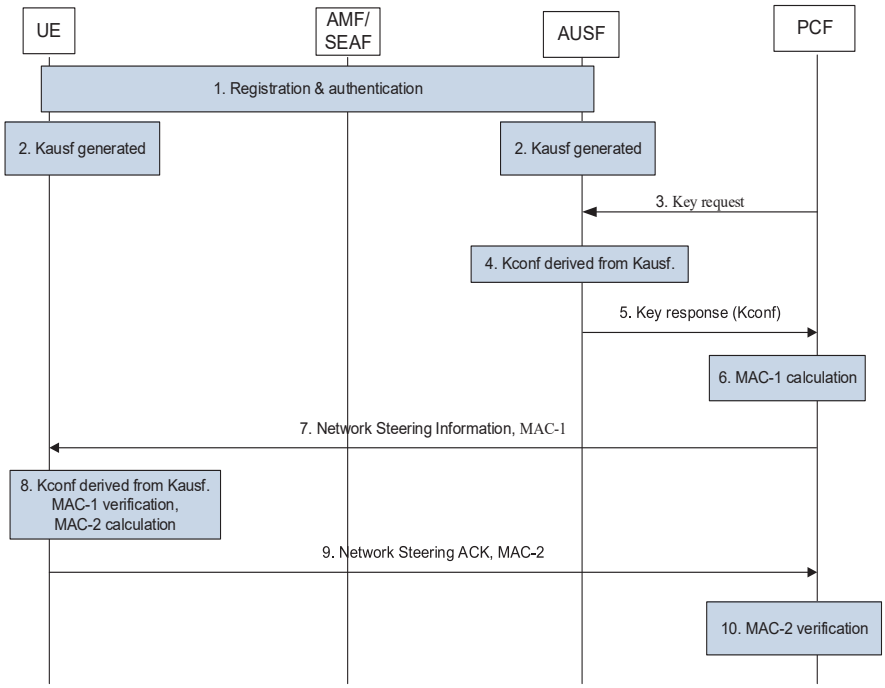

Figure 4-2: Signalling flow showing provisioning of the Network Steering Information from home PLMN to UE

1. The UE registers to the VPLMN, and is authenticated by AUSF.

2. UE and AUSF generate Kausf.

3. A node in the HPLMN (e.g. PCF) sends a key request to AUSF. This example assumes that AUSF only derives further keys from the home network root key (Kausf), and acts as an key management server, and distributes such keys in HPLMN.

4. AUSF derives the configuration key (Kconf) from the home network root key (Kausf).

5. AUSF sends the Key response with the configuration key (Kconf) to the PCF.

6. The PCF constructs the Network Steering Information, and protects it with MAC-1.

7. The PCF sends the protected Network Steering Information to the UE. There may be intermediate nodes between the PCF and the UE.

8.The UE derives the configuration key (Kconf) from the home network root key (Kausf), and verifies the MAC-1. Depending on the final protocol design, UE may send an acknowledgement message ("Network Steering ACK") to the PCF, and protect that information with the MAC-2.

9. The UE sends the protected ACK message to the PCF. There may be intermediate nodes between the node and the UE.

10. The PCF verifies the MAC-2 in the protected Network Steering ACK message.

The requirement of the UE detecting the removal of Network Steering Information by the VPLMN is very difficult to solve. This would require that the UE is able to expect such message to arrive, and AUSF would need to send the message (with the MAC) even when nothing needs to be configured. This is not efficient, and would not guarantee the delivery at any time but only when the UE expects them to arrive. Instead, we would propose the use of the acknowledge message back to the HPLMN, so that at least HPLMN is able to detect the failure of delivery.

DOCKET ALARM
Find authenticated court documents without watermarks at docketalarm.com.

4 Detailed proposal

It is proposed to send an LS back to SA2 and CT1, and report the following.

- SA3 has agreed that if end-to-end solution is required, a node in the HPLMN (e.g. AUSF or PCF) could send an integrity protected Network Steering Information to the UE. The solution would be based on the Kausf, direved from the primary authentication. This key would be known only by the UE and the HPLMN.

- The solution could be enhanced with end-to-end encryption if SA2 has a requirement of hiding the Network Steering Information from the VPLMN. Confidentiality protection over the air interface can be achieved by NAS security. However, the usage of any form of confidentiality protection may be subject to regional or national regulatory policies.

- SA3 has not found satisfactory solution for the requirement of UE detecting the removal of Network Steering Information by the VPLMN. Instead, SA3 would propose the usage of acknowledge message back to the HPLMN so that at least HPLMN knows if the UE received the information. The acknowledge information would need to be integrity protected by the UE.

DOCKET ALARM
Find authenticated court documents without watermarks at docketalarm.com.