3GPP TSG SA WG3 Security — S3#34 **S3-040577**

6 - 9 July 2004

Acapulco, Mexico

Title: **Comparison of two CRs about tunnel authentication**

Source: **Ericsson**

Document for: **Discussion and decision**

Agenda Item:

Work Item: **WLAN-IW**

1 Introduction

This paper analyzes CR S3-040493, written by NTT DoCoMo, in comparison with CR S3-040527, written by Ericsson. Both papers deal with the same interface, Wm, and offer some similarities and differences. NTT's paper deals with Wg interface as well.

As background information, the Wm interface description, taken from TS 23.234 v6.1.0, is:

> *This reference point is located between 3GPP AAA Server and Packet Data Gateway respectively between 3GPP AAA Proxy and Packet Data Gateway. The functionality of this reference point is to enable:*
>
> *- The 3GPP AAA Server/Proxy to retrieve tunneling attributes and WLAN UE's IP configuration parameters from/via Packet Data Gateway.*
>
> *- Carrying messages between PDG and AAA Server in support of the user authentication exchange which takes place between WLAN UE and 3GPP AAA server/proxy.*
>
> *- Carrying messages for user authorization between PDG and 3GPP AAA server/proxy.*
>
> *- Carrying authentication data for the purpose of tunnel establishment, tunnel data authentication and encryption.*
>
> *- Carrying mapping of a user identifier and a tunnel identifier sent from the PDG to the AAA Proxy through the AAA Server.*

On the other hand, Wg interface description in TS 23.234 states:

> *The Wg reference point applies to WLAN 3GPP IP Access.*
>
> *This is an AAA interface between the 3GPP AAA Server/Proxy and the WAG. It is used to*
>
> *- Provide information needed by the WAG to perform policy enforcement functions for authorised users.*
>
> *- Transport per-tunnel based charging information from the WAG to the AAA Proxy.*

2 Discussion

As a general comment, NTT repeats the full EAP AKA authentication process with all the details, which is not needed as it is already in other parts of the TS. This will make difficult the track of changes if the EAP SIM/AKA processes are modified. In Ericsson's CR it is just stated that the whole EAP process is described in other chapter, in order to avoid repetition, and the EAP procedure is summarized as much as possible. Only the relevant aspects of the EAP procedure are described.

On the other hand, NTT's CR adds the control of simultaneous sessions in the EAP authentication process, which is missing in Ericsson's CR. It is right that this part has to be present in the EAP authentication procedure, but it should be studied more in detail how it is performed. For example, in NTT's CR it is written that the VPLMN id is sent but currently in EAP over IKEv2 there is no way to convey such information.

More specific comments are detailed below:

- Step (3) in NTT's CR states that the IMSI or the pseudonym is sent. In Ericsson's CR it's only the IMSI because the message in which the IMSI is sent is encrypted.

- Step (3) in NTT's CR, the 3GPP AAA server number is sent. The idea is good, because in case of a pool of 3GPP AAA servers, it will indicate the PDG which AAA server has to communicate with, but the problem is that there is no way to transport that information in EAP or IKEv2. Furthermore, the AAA server number is unknown for the WLAN UE.

- Step (4) in NTT's CR does not include the indication of the type of authentication, as there is in Ericsson's CR in step (3)

- Step (4) in NTT's CR, the VPLMN id and WLAN radio network id are sent. As commented before, there is no way to insert that information in the IKEv2 message of EAP payload. Currently this is carried out with RADIUS and Diameter.

- Step (4) in Ericsson's CR says that the HSS will check for authorization of the user to establish the tunnel. Although authorization is something different to authentication, this checking is inherent to the complete EAP process and it is included for completeness.

- Steps (5,6,7) in NTT's CR can be omitted (or summarized), as commented before. They are not needed in as they are already in the full authentication procedure

- Step (5) in Ericsson's CR mentions why the identity is not needed to be re-requested. This aspect is not covered by the NTT's CR

- Steps (9, 10) in Ericsson's CR describes how the AUTH payload is generated using the MSK and why the AUTH is calculated. It is explained as well how the MSK is transferred from the AAA server to the PDG. Those aspects are missing in step (15) of NTT's CR.

- Step (20) in NTT's CR does not describe how the IKE_INIT messages are authenticated in the last phase of the IKEv2 exchange. Those actions are described in Ericsson's CR steps (11, 12)

- Step (21) in NTT's CR defines some actions about simultaneous access. As commented previously, this is not clear how to perform simultaneous access, as there are some parameters which can not be sent in the EAP authentication, and should be left for further study.

Comments similar to the previous ones are applicable to the fast re-authentication procedure.

On the other hand, NTT describes as well flows between the AAA and the WAG, the Wg interface. The Wg interface, as described in TS 23.234, is used to convey policy and filtering information, but not for authentication purposes. So the relationship of this interface with security-related functions is questionable.

Apart from that, there are some issues still unresolved about Wg interface, for example:

- What happens if there is a NAT between the WAG and the PDG ?

- What does this filtering policy consists of ?

3 Conclusions

According to the previous analysis, it is proposed to adopt Ericsson's CR for Wm interface description. However, there are still some open issues to be addressed:

- Simultaneous access control when authenticating in scenario 3. Covered in NTT's CR but still needs to be studied in detail

- Re-authentication procedure for scenario 3 has to be added to TS 33.234. Covered in NTT's CR but some corrections have to be performed, as indicated in the analysis above.

About the Wg interface description, this interface is not security-related and should be left for other groups.