3GPP TSG SA WG3 Security — S3#29 **S3-030369**
15-18 July 2003
San Francisco, USA

~~**3GPP TSG SA WG3 Security — S3#28** **S3-030261**~~
~~**6 - 9 May 2003**~~
~~**Berlin, Germany**~~

Agenda Item: WLAN

Source: Ericsson

Title: WLAN – Implications of the trust relation between the Cellular Operator and the WLAN Access Provider

Document for: Discussion and decision

1. Introduction

This document considers the trust relation between the Cellular Operator and the WLAN Access Provider (see Annex B of TS33.234) and analyses how this trust relation impacts on the WLAN-3GPP interworking solution.

The contents of this document are the result of a contribution originally sent by Ericsson plus some modifications as consequence of an e-mail discussion in SA3 mailing list. Some conclusions of the discussion are:

- Ericsson intention is to have the trust model in the informative part of the TS, as a basis for future discussions. If some of these conclusions are wanted to be taken as normative, Ericsson proposal is to write separate contributions in order to have them in the normative part.
- There have been a few comments about why SA3 is writing about charging. Again, this is not a normative text, and the charging issues reflected in the paper are used in order to figure out the implications of each trust situation when reporting charging information and the possible risks.
- The different types of tunneling we can now list (tunnel without protection, origin authentication and integrity, etc.) deserve a separate analysis, which in Ericsson opinion should be performed when scenario 3 is more stable in SA2. At the moment we refer to it as tunneling in general.
- Some companies (AWS and Mobility Networks) expressed their disagreement with the topic under discussion, specially because their opinion is that SA3 is not adhering to SA2 architectural decisions. With this contribution, SA3 is not taking any decision about architecture, and tries to define a trust model as much generic as possible so that it can fit in SA2 current specifications.

Some topics raised during the discussion are not covered in this contribution but they are a very valuable input for future contributions:

- Trust model split for user data and signalling
- Security related to charging information (I guess this would require cooperation with SA2 and SA5)
- Mapping of trust levels to scenarios defined in SA2 (I suppose this will happen when scenarios are more stable)

2. Assumptions

For simplicity, only two levels of trust are considered between the Cellular Operator and the WLAN Access Provider:

- Low trust: The Cellular Operator does not trust the WLAN Access Provider so much as to base charging only on accounting records received from the WLAN Access Provider. Moreover, the Cellular Operator cannot count on the WLAN Access Provider Network to perform actions such as authorisation enforcement, WLAN session tear down, etc. at demand of the Cellular Operator Network.
- High trust: The Cellular Operator trusts the WLAN Access Provider so much as to base charging on accounting records received from the WLAN Access Provider, and to relay tasks (such as authorisation enforcement, WLAN session tear down, etc.) on the WLAN Access Provider Network.

Additionally, two groups of ~~scenarios~~ services are considered with regard to the implications of the trust relation between the Cellular Operator and the WLAN Access Provider:

- Access to services provided by the WLAN Access Provider, which corresponds to scenarios 1 and 2 described in ref. [1]. These services are WLAN technology specific.
- Access to services provided by the Cellular Operator. This corresponds to scenarios 3, 4, 5 and 6 in ref. [1]. These services are the ones typically offered by 3GPP networks.

3. Implications of Low Trust between the Cellular Operator and the WLAN Access Provider

3.1 Access to services provided by the WLAN Access Provider

In this scenario, user traffic does not get to the Cellular Operator Network, and accounting information received from the WLAN Access Provider cannot be trusted. The only reliable information that the Cellular Operator has about its subscribers getting WLAN services from the WLAN Access Provider is authentication information, which probably is not sufficient to carry out charging based on usage. E.g. it can be known when a WLAN session begins but not when it ends. Therefore, ~~it is likely that the subscriber will have to be charged based on some fee not depending on usage.~~it maybe risky for the operator to perform charging based on usage or volume.

Moreover, the Cellular Operator Network can send authorisation directives to the WLAN Access Provider Network, but it cannot count on the WLAN Access Provider network actually enforcing authorisation according to those authorisation directives. Therefore, ~~the subscriber should not be charged based on the authorisation level.~~charging based on authorization may not correspond to the services the subscriber is using in reality.

Also, in this case the Cellular Operator has no means to ensure protection of user data.

3.2 Access to services provided by the Cellular Operator

User data arrives to the Cellular Operator Network, thanks to tunnels between the WLAN-UEs and the Cellular Operator Network. Charging, authorisation enforcement, control of sessions, etc. must be carried out at the Cellular Operator Network, taking the necessary actions on traffic received from the users via the aforementioned tunnels.

Furthermore, the tunnelling mechanism must be able to provide protection of user data, at least data origin authentication and integrity protection.

4. Implications of High Trust between the Cellular Operator and the WLAN Access Provider

4.1 Access to services provided by the WLAN Access Provider

User traffic does not get to the Cellular Operator Network, but the subscriber can be charged based on accounting information received from the WLAN Access Provider.

Moreover, the Cellular Operator Network may control sessions, authorisation, etc. by exchanging information with the WLAN Access Provider Network.

The WLAN Access Provider is trusted to grant adequate protection of user data.

4.2 Access to services provided by the Cellular Operator

The subscriber can be charged based on information available at the Cellular Operator Network and/or information available at the WLAN Access Provider Network. Likewise, authorisation enforcement, control of sessions, etc. can be performed with participation of both networks.

If the WLAN Access Provider provides sufficient protection of user data and there is an acceptable security level between the WLAN Access Provider and the Cellular Operator (e.g. with NDS/IP), it may be unnecessary to implement any protection mechanism in the tunnel between the WLAN-UE and the Cellular Operator Network.

5. Conclusions

The following table summarises the conclusions of the present analysis.

	LOW TRUST	HIGH TRUST
Access to services provided by the WLAN Access Provider	• ~~Subscriber should not be charged~~ Charging based on usage or authorisation level.maybe risky for the Cellular Operator, the accounting information may be not reliable. • Cellular Operator cannot grant user data protection.	• Cellular Operator controls sessions, charging, authorisation, etc., based on information received from the WLAN Access Provider Network, and actions performed at said network. • The WLAN Access Provider is trusted to grant adequate protection of user data.
Access to services provided by the Cellular Operator	• Charging, authorisation enforcement, control of sessions, etc. must be performed at the Cellular Operator Network, counting on user data received via tunnels. • The tunnelling mechanism must be able to provide data origin authentication and integrity protection at least. • The tunnelling mechanism may have as end point either the HPLMN or the VPLMN, depending on some aspects e.g. the need to access services in the VPLMN	• Charging, authorisation enforcement, control of sessions, etc. can be performed with participation of both networks. • It may be unnecessary that the tunnelling mechanism implements any protection mechanism~~.~~, if there is protection of user data in the WLAN AP and there is some security mechanism between the WLAN AP and the Cellular Operator.

It is suggested to incorporate this analysis into Annex B of TS 33.234.

It is also proposed that SA3 informs SA1 and SA2 about the implications that the trust relation between the Cellular Operator and the WLAN Access Provider has on the WLAN-3GPP interworking solution.

6. References

[1] 3GPP TR 22.934 "Feasibility study on 3GPP system to Wireless Local Area Network (WLAN) interworking"