3GPP TSG SA WG3 Security — S3#29 **S3-030332**
15 - 18 July 2003
San Francisco, USA

Source: **BT Group**

Contact: **Colin Blanchard colin.blanchard@bt.com**

Title: **Alternative WLAN Inter-working Trust Model**

Document for: **Discussion and decision**

Agenda Item: **WLAN**

Abstract

This contribution purposes some modifications to the trust model suggested by Ericsson in S3-03026 to reflect the comments made on the SA3 list since SA3#28 specifically that:

- *The definition of services and how those are charged is outside the remit of SA3. SA3 can, however, point out how the risk to the network operator is impacted by the S5 decisions on charging and the inter- working scenarios defined by SA2*
- *SA3 may need to specify an encrypted and integrity-protected tunnel from the UE to the home, together with a suitable key management procedure.*

This contribution shows how the risk for a given charging and level of trust in a partner network may be managed. This is through an appropriate (e.g. with a defined level of Assurance) series of recommendations for operational procedures such as credit checks and terms and conditions in roaming agreements.

**********Start of Original Text from Ericsson (contribution S3-03026)**********

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.

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. In a low trust relation, the end user may wish to provide locally managed “end to end overlay security” solution.
- 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. In a high trust relation, the end user may not

require any further protection for their data or will trust the operator to provide a centrally managed “end to end overlay security” solution.

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].
- Access to services provided by the Cellular Operator. This corresponds to scenarios 3, 4, 5 and 6 in ref. [1].

Services may employ different charging principles e.g. a “free” service at one extreme, to a per volume per service invocation at the other extreme, with flat rate charging being typical for many services

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

With this group of services ~~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.

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.

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, it may be unnecessary to implement any protection mechanism in the tunnel between the WLAN-UE and the Cellular Operator Network.

**********End of Original Text from Ericsson (contribution S3-03026)**********

**********Start of new Text **********

5 Conclusions

Any current or planned service within the scenarios defined by SA2 can be at considered as the intersection between:

1. A point defined by the level of trust on an axis that has no trust at one extreme to complete trust at the other extreme.
2. A point defined by the charging principle employed by the service e.g. "free" service at one extreme, to a per volume per service invocation at the other extreme, with flat rate charging somewhere in the middle.

This is shown in figure 1, and gives a view of the level of business risk to the network operator in terms of billing disputes, fraud losses that will increase as services that contain a higher proportion of volume based charging, are run over lower trust networks.

Even with free services, there may be an issue with managing capacity, e.g. if some people are using all the capacity on system by setting up many permanent calls then some procedure with an specific assurance level will be needed to "kick them off" that does not assume high trust in the WLAN.

A similar view of risk, but this time from the perspective of the end user, to the confidentiality and integrity of their personal data, can also be considered. (Figure 2) This time, the extremes on one axis are access to public information, with no concern over privacy of use of the service at one end, and the financial transactions at the other. The extremes of the other axis, are full trust placed in network operator to manage security configuration and encryption keys to a locally managed "end to end overlay security" solution at the other.

Since in practice in 3GPP the architecture and charging principle are outside the control of SA3, SA3 can only seek to manage this risk by defining an appropriate level of assurance needed in the design and operational procedures. Some example are given in the table below, but SA3 would need identify the actual recommendations and complete the table

Assurance Level Indication	**Recommendations to Network Operator**	**Recommendations to end user**
3.3		
3.3		
3.1	Re-authenticate every hour Bilateral roaming agreement shall require the use of NDS/ IP to secure…	Locally managed "end to end overlay security solution"
3.0	Re-authenticate every 24 hrs	

2.3		
2.2		
2.1		
2.0		
1.3		
1.2		
1.1		
1.0		
0.3		
0.2		
0.1		
0	None	None

Figure 1 Control Plane Trust Model

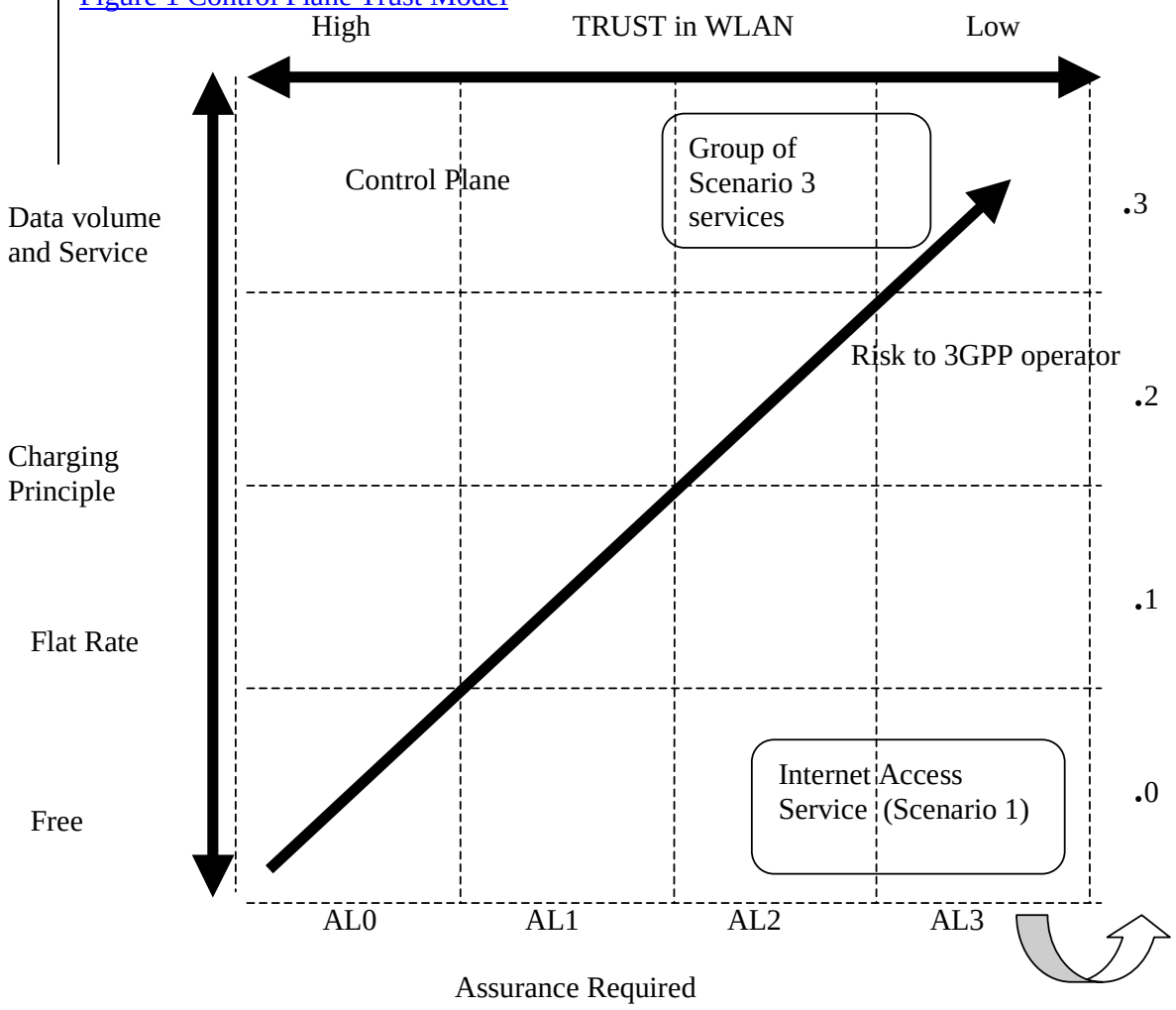

Figure 2 User plane Trust Model