3GPP TSG SA WG3 Security — S3#26 **S3-020608**
19- 22 November 2002
Oxford, UK

Agenda Item:

Source: Orange France

Title: Pseudo CR to requirements for WLAN interworking with 3GPP

Document for: Discussion and Approval

1. Introduction

In SA3 last plenary meeting in Munich, the draft TS for WLAN interworking was briefly reviewed, and the group agreed that the section on requirements required some important editing, because it contained many requirements that were not security related. Furthermore, SA2 had a meeting the week after last SA3 plenary and edited TS 23.234, removing all security requirements from that document. A liaison statement (S2-023122) was sent to SA3 to inform us we need to make sure security requirements are properly addressed in our TS.

The proposal at the bottom of this document is to remove many of the listed requirements that were either non security related or too vague. Basically the thinking behind our proposal is the following:

- Authentication shall be based on the SIM/USIM, it provides us with a security module that is perfectly fitted for our needs
- Authentication mechanism should also provide key agreement as it is done in GSM and UMTS. Key material can afterwards be used by the security mechanisms of each underlying WLAN radio technology (encryption, integrity...)
- No clear requirement is given on the security mechanisms to be applied to the WLAN radio interface. We suggest to remove the notion of “equivalent security level” for anything that is not authentication mechanism. The main reason is that while we can ensure features in the authentication mechanism since it is under the control of 3GPP, it is not possible to make assumption on security provided by the underlying radio access technology. It remains an open issue whether SA3 wants to mandate additional requirements, but clearly, SA3 requirements cannot realistically impact WLAN radio access standards. It may be interesting to study possibilities to add security at an upper layer like Ericsson suggested in S3-020539. However, there are difficulties with such proposals and these should be studied further and proven doable in order to avoid including a requirement that would not be technically feasible.

4.2 Security Requirements

[Editor's note: These requirements are copied from TS 23.xxx v0.1.0 for the first version of this TR, and shall be reviewed and updated according to the input from the preceding sections]

~~- Legacy WLAN terminals should be supported.~~

~~- Minimal impact on the user equipment, i.e. client software.~~

~~- The need for operators to administer and maintain end user SW should be minimized~~

~~- Existing UICC cards should be supported. The solution as such should not require any new changes to the UICC cards.~~

~~- Changes in the HSS/HLR/AuC should be minimized.~~

~~- The security data, i.e. long-term keys, which are stored on the UICCcard must not be sent from the card itself. Instead the interface to the UICC card should be of type challenge-response, i.e. a challenge is sent to the UICC card and a response is received in return.~~

~~- The user should have same security level for WLAN access as for 3GPP access.~~

~~- Mutual Authentication should be supported~~

~~- The selected Authentication solution should also allow for Authorisation~~

~~- Methods for key distribution to the WLAN access NW shall be supported~~

- Selected WLAN authentication mechanisms for 3GPP interworking shall provide at least the same security features as 3GPP System authentication procedure. It shall make use of the existing application(s) residing on the UICC card. Mutual authentication between the home network and client shall be supported.

- It shall be possible to store all long-term security credentials used for subscriber and network authentication in a tamper resistant memory such as the UICC card.

- The security data, i.e. long-term keys, which are stored on the UICCcard must not be sent from the card itself. Instead the interface to the UICC card should be of type challenge-response, i.e. a challenge is sent to the UICC card and a response is received in return.

~~- Subsequent WLAN re-authentication shall not compromise the requirement for 3GPP System equivalent security~~

- Selected WLAN Authentication mechanisms for 3GPP interworking shall support agreement of session keying material which shall be used by security mechanisms in the WLAN radio interface

~~- Selected WLAN key agreement and key distribution mechanism shall be secure against man in the middle attacks. In other words, a man in the middle shall not be able to learn the session key material.~~

~~- The WLAN technology specific connection between the WLAN UE and WLAN AN shall be able to utilise the generated keying material for protecting the integrity of an authenticated connection~~

~~- It shall be possible to store all long-term security credentials used for subscriber and network authentication in a tamper proof resistant memory such as the UICC card.~~