3GPP TSG SA WG3 Security — SA3#35 **S3-040726**

October 5-8, 2004

St Paul's Bay, Malta

Response to Ericsson, Nokia's Discussion paper by Toshiba (see blue Text)

Title: **Classification of security requirements on local interface**

Source: **Ericsson, Nokia**

Document for: **Discussion and decision**

Agenda Item: **6.10**

Work Item: **WLAN-IW**

1 Introduction

This document is for discussion on the conference call. The comments are inserted in blue colour.

The red text indicates the results of the conf. call dated September 16th 04.

In 3GPP SA3 #34 meeting there was a CR provided by Toshiba, etc on (U)SIM security re-use. Some generic security requirements on local interface were discussed in the later conference calls. However a classification is needed to justify whether a requirement is right to appear in 33.234, or it's better to be addressed in other standardization organization.

2 Discussion

2.1 The generic classification criteria:

- Since 33.234 is on WLAN interworking security, the requirement should be related to WLAN and related to security.
- The requirements to be in TS 33.234 should be feasible to realize in release 6 timeframe. If not, they should be left out for release 7 (as it does not make sense to have requirements without a technical solution in a TS)

Please refer to Chairman TSG SA's report to PCG No. 3GPP/PCG#12(04)05 dated May 2004 section 6 which says that "TSG SA has decided to "freeze" Release 6 in terms of requirements except for items already identified" And not in term of realization of requirements.

Ericsson suggested asking SA for clarification. Since the discussion was quite constructive I believe it is no longer needed.

- The generic security requirements on local interface should be used on all kind of local interface, e.g. Bluetooth, Infrared, etc, but not on a special interface.
- The security requirements on a special interface may be as an informative annex.

- The requirement should be on devices' function, but not on user's capability.

Necessary wordsmithing has been done by Nokia. (Comment has already been addressed over previous conf call).

Nokia suggested to double check the requirement.

- If the requirement has been addressed in other standardization organization, it shouldn't be in 33.234 to avoid overlapping. For example, OMA has work on device management.

2.2 Modification on S3-040627 and S3-040628

This classification refers to the requirements of S3-040627. It is specified when it relates to the requirements of S3-040628.

Redundant requirements

- Integrity and privacy of signalling between the WLAN system, the 3GPP core network, and the WLAN-UE shall be supported. Leakage of (U)SIM information (authentication data, session keys) to the user, or any third party over the wireless interface (Bluetooth/WLAN) is the major security threat. This leakage of information shall be guarded against.

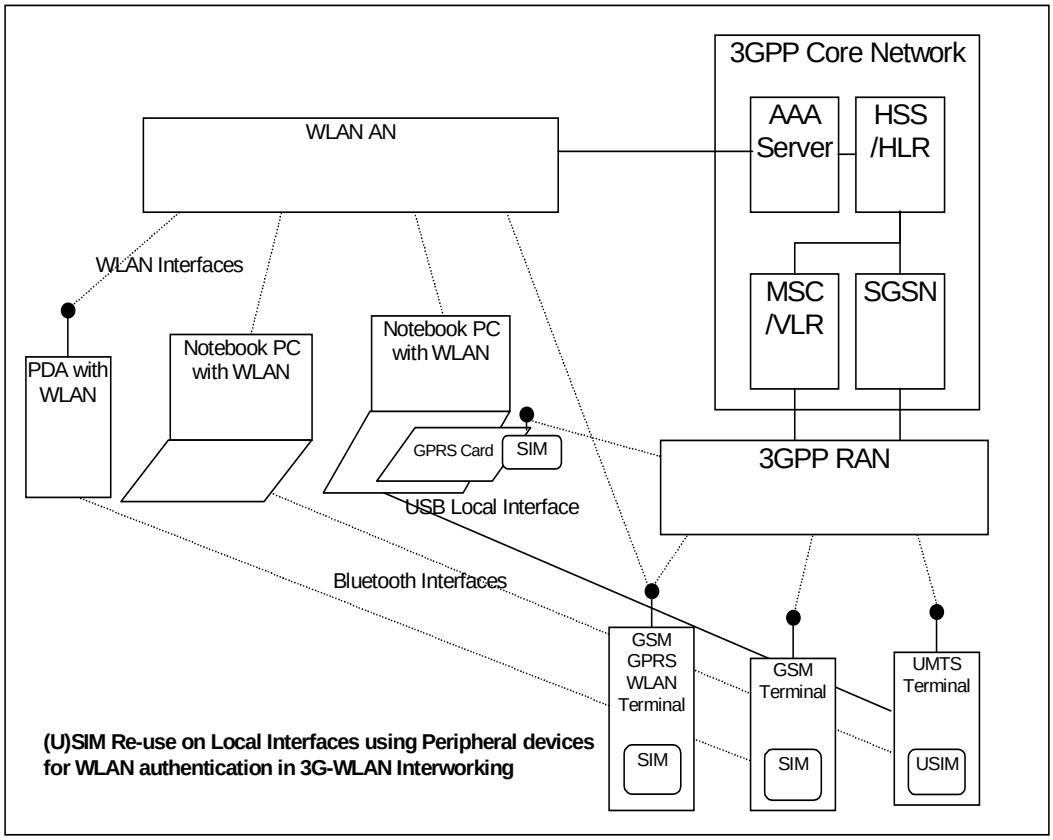
  This is already covered in the requirement:

  - Protection should be provided for WLAN authentication data and keying material on the Wa, Wd and Wx interfaces.

  except the interface WLAN UE-WLAN network, which is not under 3GPP scope.

This requirement is misunderstood. Please refer the Figure 1 of TR-33.817. In this requirement neither Wa, Wd, Wx are under consideration but the local interface between split UE is under consideration. Thus Leakage of (U)SIM information (authentication data, session keys) to the user, or any third party over split UE interface shall be guarded against.

Above comment was accepted. Stefan (T-Mobile) suggested that we specify that Wa, Wd, Wx are addressed some where else.



NOTE: The figure shows several different scenarios and does not necessarily mean that all the devices shown in the figure are accessing simultaneously using single (U)SIM.

Figure 1: (U)SIM Security Re-use by Peripheral Devices Using Local Interfaces (USB/BT, etc.)

Non-security requirements

- It shall be possible to simultaneously access both WLAN and 3GPP radio access technologies. I.e., It shall support simultaneous calls on two different air interfaces. For example, the UE might use the WLAN for data services (internet access) together with the 3GPP system for a speech call.

  This is not a security requirement. It's already covered in 23.234:

  - The WLAN connection established for a 3GPP subscriber shall have no impact to the capabilities of having simultaneous PS and CS connections for the same subscriber.

It is a functional requirement, yet it needs to be communicated to Bluetooth-SIG because SAP in Bluetooth SIG may need enhancement for the a single (U)SIM to support simultaneous calls on two different air interfaces.

Stefan, Selim (Intel) and Holger (Axalto) wanted to check and confirm this.

Requirements in other standardization organization

- UICC presence detection according to [34] shall be supported via the local interface. This mechanism ensures that the UICC has not been removed during a card session. Thus every component of the functionally split WLAN-UE issues a STATUS command every 30 seconds to detect UICC presence during a call. [34] requires that in case no response data is received to this STATUS command, then the call is terminated within 5 seconds after the STATUS command has been sent. If the local interface utilizes a radio link (e.g. Bluetooth), it may encounter severe interference that prevents UICC presence detection. This will result in a drop of the ongoing WLAN session. The UICC presence detection of functionally split WLAN-UE should be able to cope with such problems, e.g. by retransmission of the STATUS command for a limited amount of time.

This is more a feature description than a requirement. It should be where the ref. [34] is.

It was suggested to provide the reference for USIM as well. Moreover Holger suggested keeping the requirement, but changing the highlighted text above "Thus every component" to "In particular TE"

Please refer to 3GPP TS 11.11 that explains the mechanism how SIM misuse can be protected.

"As an additional mechanism, to ensure that the SIM has not been removed during a card session, the ME sends, at frequent intervals, a STATUS command during each call. A STATUS command shall be issued within all 30 second periods of inactivity on the SIM-ME interface during a call. Inactivity in this case is defined as starting at the end of the last communication or the last issued STATUS command. If no response data is received to this STATUS command, then the call shall be terminated as soon as possible but at least within 5 seconds after the STATUS command has been sent. If the DF indicated in response to a STATUS command is not the same as that which was indicated in the previous response, or accessed by the previous command, then the call shall be terminated as soon as possible but at least within 5 seconds after the response data has been received. This procedure shall be used in addition to a mechanical or other device used to detect the removal of a SIM".

Thus it may not be considered as a feature but a requirements that calls for the enhancement of this mechanism to protect misuse of (U)SIM.

- The peripheral device without (U)SIM shall be capable of communicating with the U(SIM) only if the device containing (U)SIM is switched on and a (U)SIM is powered on. Furthermore the device without (U)SIM shall not be allowed to change the status of the device with (U)SIM, or the (U)SIM, e.g. to reset it, or to switch its power on or off.

Should this be sent to T groups ?

If we document this requirement in 33.234, T group can work on the mechanism.

It was decided to delete the highlighted text only and keep the requirement.

- The peripheral device without the (U)SIM shall be capable of detecting the presence and availability of the (U)SIM on the device containing it.

- It shall also have the ability to terminate an authenticated network sessions when, the (U)SIM is no longer accessible within a short monitoring time period as defined in TS 31.102 [33]. Remove when

Should this be sent to T groups ?

If we document this requirement in 33.234, T group can work on the mechanism.

It was decided to keep the requirement and replace the highlighted text "Presence and availability" with "accessibility".

Candidate requirements to be in TS 33.234, but without a technical solution in release 6 timeframe

- Applications/Data information could be retrieved from (U)SIM, provided that (U)SIM is inserted in a 3GPP ME. When the (U)SIM is re-used over local interfaces, further access control on the Applications/Data information shall be applied by the 3GPP ME holding the (U)SIM.

There is currently no technical description of this feature in TS 33.234

- (U)SIM Security Reuse shall be consistent with current security arrangements for Release 6 and ensure that user security is not compromised.

How can this requirement be realized technically ?

TSG SA has decided to "freeze" Release 6 in terms of requirements as noted above.

Security requirements on a special interface

Requirements in chapter 4.2.4.3 should be moved to an Annex.

Should be communicated to Bluetooth SIG under liaison as agreed in previous SA3 meetings, that resultant requirement swill be send to Bluetooth SIG.

Requirements in 040628 should be moved to an Annex

Stefan, Selim and Holger (Axalto) wanted to check and confirm this and send their guidance.

3 Conclusions

The classification should be used to justify the requirements in S3-040627 and S3-040628. Section 4.2.4.3 in S3-040627 should be moved to Annex. Requirements in 040628 should be moved to an Annex

Call terminated before reaching this part.

4 References

[34] 3GPP TS 51.011: "Specification of the Subscriber Identity Module – Mobile Equipment (SIM – ME) Interface".