3GPP TSG SA WG3 Security ó SA3#35 **S3-040840**
October 5-8, 2004
St Paul's Bay, Malta

Title: Draft LS on EAP Authentication commands for WLAN interworking
Response to: -
Release: Rel-6
Work Item: WLAN Security

Source: SA3
To: T2
Cc: T3

Contact Person:
Name: Stefan Schrˆ der
Tel. Number: +49 228 936 33312
E-mail Address: stefan.schroeder@t-mobile.de

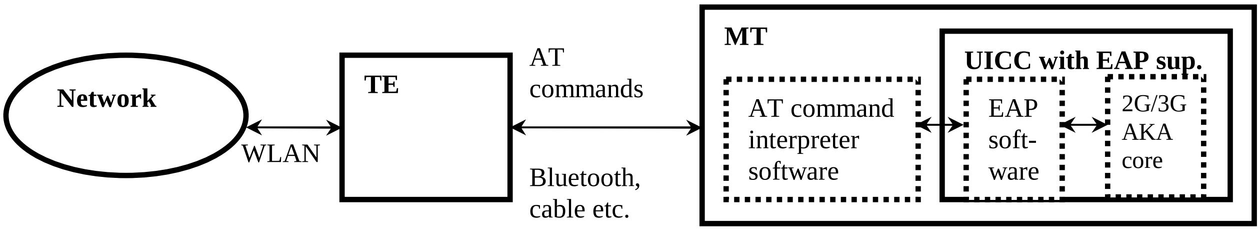
Attachments: S3-040841

1. Overall Description

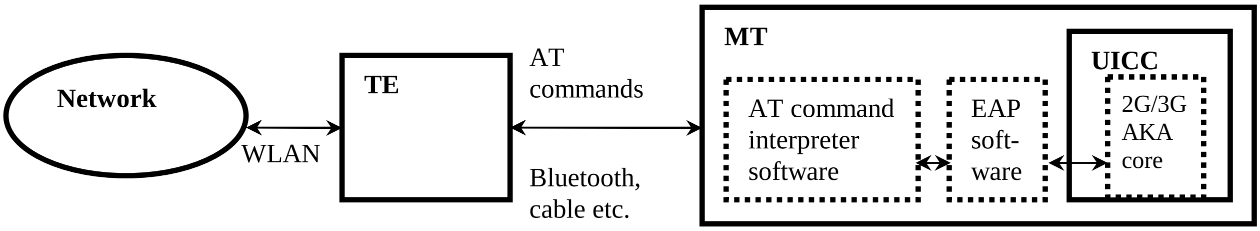
1.1 WLAN authentication

SA3 discussed solutions to achieve authentication for WLAN access with a functionally split WLAN-UE. In the configuration considered, the WLAN-UE is functionally split into two physical devices that securely communicate over a local interface, e.g. Bluetooth, or serial cable. One device may be a laptop computer with WLAN card (TE), the other one a mobile phone with a UICC or SIM (MT).
Authentication takes place using EAP-SIM or EAP-AKA. SA3 decided that EAP must terminate inside the MT, in order not to leak any 2G/3G keys out to the TE. Therefore, two different implementations exist, depending on the location of EAP support:

1. If the UICC supports EAP according to ETSI TS 102.310, and the MT supports the appropriate filter rules to prevent illegitimate commands to the card, EAP is run on the card:



2. If the UICC or SIM card does not support EAP, the MT must run EAP, and use standard 2G/3G authentication commands towards the card:



For implementation 1, the AT commands "Restricted UICC Logical Channel access +CRLA" and "Generic UICC Logical Channel access +CGLA" according to TS 27.007 can be used, as proposed in S3-040760 (related CR is attached). However, it was pointed out during the discussion at SA3#35 that the use of these commands may pose a security risk, as the security depends on the presence of appropriate filtering rules in the MT to prevent that the TE sends arbitrary commands to the card. For implementation 2, it is not yet defined which commands to use.

SA3 currently sees the following possibilities:

A) T2 could change TS 27.007 so that the existing AT commands mentioned above could be re-used for UICC and SIM cards without EAP support in implementation 2. This could be done by adding to the text of sections 8.18 and 8.44 of TS 27.007 that the AT commands may also be used to allow the TE to send commands to applications on the MT outside the UICC or SIM. In that case, the MT would only forward the EAP authentication commands to the card in case the card supports EAP and the filter rules are in place. Otherwise the applications on the MT would handle EAP.

B) T2 could define new AT command(s) dedicated to transferring EAP authentication messages only. The MT would then run the commands mentioned above towards the card, if the card supports EAP. Otherwise the applications on the MT would handle EAP.

Option A) has the advantage that not much specification work is needed. It has, however, the security disadvantage that it opens a direct channel from the TE to the smart card. Therefore, option A)'s security depends on the quality of filtering measures implemented in the MT to drop any command to the card which is not used for EAP authentication, whereas Option B) strictly limits the TE's possibilities to EAP authentication.

It was also pointed out at SA3#35 that it is highly desirable to have a unified procedure for both, cases 1 and 2. It shall not be required that the TE is aware of the particular function split in the MT. Therefore the TE shall use the same commands in both cases.

1.2 Risks of direct UICC access by the TE

Independent from the above topics, SA3 is concerned about the AT commands that give a TE full access to the smart card. SA3 considered the risks of 2G/3G authentication data leakage into an open platform like a PC-based TE, and decided that this leakage must be avoided. The open platform could be infected by Trojan Horse software that supports remote cloning attacks against the unsuspecting subscriber. Therefore, SA3 found it necessary to terminate EAP in the MT, so that only the EAP keys for WLAN authentication are given out to the TE.

These efforts are useless if they can be circumvented by a powerful command like "Generic access", which allows the TE to arbitrarily run Authenticate commands to the card in GSM or 3G context. Therefore, SA3 considers it necessary to prevent illegal or accidental use of the "Generic access" command by restricting access to it, e.g. by following measures:

C) In the default MT state after power-up, the "Generic access" command, if received via a TE-MT interface, shall be protected by a mandatory lock. TS 27.007 V6.6.0 currently defines the lock on the "Generic access" as optional.

D) If option A) is selected by T2, the "Generic access" command shall additionally support a "half-unlocked" state, where only the EAP commands are passed through to the UICC, but all other commands are blocked by a filter in the MT, which analyzes the "Generic access" command contents.

2. Actions

ACTION1: SA3 kindly asks T2 to consider options A) and B) above, and possibly other solutions, and implement the required functionality within Rel-6 time frame. It would also be appreciated if T2 could indicate that a unified solution was seen as possible, but not in the Rel-6 timeframe.

ACTION2: SA3 kindly asks T2 to address SA3's concerns pointed out in section 1.2, e.g. by mandating a secure lock mechanism on the "Generic access" command.

3. Date of Next TSG-SA3 Meetings

SA3#36	23 - 26 November 2004	Shenzhen, China
SA3#37	21 - 25 February 2005	Sophia Antipolis, France