3GPP TSG-T (Terminals) Meeting #9
Hawaii, USA, 20 - 22 September, 2000

Tdoc TP-000122

Technical Specification Group Services and System Aspects

TSGS#8(00)353

Meeting #8, Düsseldorf, Germany, 26-28 June 2000

Source: **Ad hoc UE Split Group**
Document for: **Approval**
Agenda Item: **Postponed Items**

LIAISON STATEMENT

From: **TSG-SA**

To: **GSM Association, S1, S2, S3, S4,**
EICTA CelCom, GSM Certification Forum

Cc: **TSG-T, T2**

TSG-SA has discussed the attached paper (SP-000313) which highlights some issues and concerns associated with providing call control applications in one or more attached external devices routing calls through an ME.

The opinion of TSG-SA is that this area has not been fully studied to date and it is important to understand which scenarios should be examined in further detail. TSG-SA will revisit this subject once further information is available from the groups addressed above.

The attached document discusses several scenarios, some of which are raised by more immediate technical concerns and some of which are issues of principle.

Of immediate concern is the UE requirement to support multiple data streams. TSG-SA sees a need to establish clear requirement scenarios and would appreciate feedback on this issue, e.g. the support of multiple PDP contexts.

On the issues of principle, TSG-SA#8 recognises the Industry developments in the direction of providing PC-based multimedia clients. TSG-SA is prepared to discuss this at future meetings. However, TSG-SA#8 is not ready to accept the proposal to provide call control applications in one or more attached external devices and routing calls through an ME; feedback on the full implications of this proposal is welcomed from the addressed groups. TSG-SA has serious concerns including the following specific issues:

- Validity of the mutual authentication between the user and the network
- Termination point for the ciphering and integrity checking
- IMEI location and security
- Validity and scope of conformance testing
- PC virus attacks
- Malicious tampering with software located in the PC
- Misuse of open connections by third parties
- Fraud (e.g. theft of service)

All of the above items imply that there is a set of functionality that should not be split.

TSG-SA notes that the 3G system is highly reliant on all relevant components being fully interoperable and secure. Therefore TSG-SA believes that 3GPP needs to be involved in the development of any relevant protocols which have an impact on the 3GPP system, including those which work between an ME and a physically separate TE. TSG-SA believes that there is a serious risk to the integrity and stability of the 3GPP system unless all relevant protocols are brought into the discussion in appropriate 3GPP groups.

We therefore invite the GSM Association and EICTA CelCom to consider this matter and identify what the market requirements would be for providing Mobile Multimedia and other services using devices outside of the UMTS radio handset.

Product testing and certification including IMEI security are believed to be potential problem areas, hence the GSM Certification Forum is also invited to consider the implications.

S1 is asked to study the requirements for supported scenarios.

S2 is asked to identify any architectural impacts

S3 is asked to identify security issues

S4 is asked to comment on the scenarios currently considered/included in Release 99 and provide also a view for Release 2000.

In order to help develop this work in harmony, it would be useful to copy any responses to all those on the To: and Cc: lists above.

3GPP TSG-SA Meeting #8
Düsseldorf, Germany, 26 - 28 June, 2000

Tdoc SP-000313

3GPP TSG-T (Terminals) Meeting #8
Düsseldorf, Germany, 21 - 23 June, 2000

Tdoc TP-000115

LIAISON STATEMENT

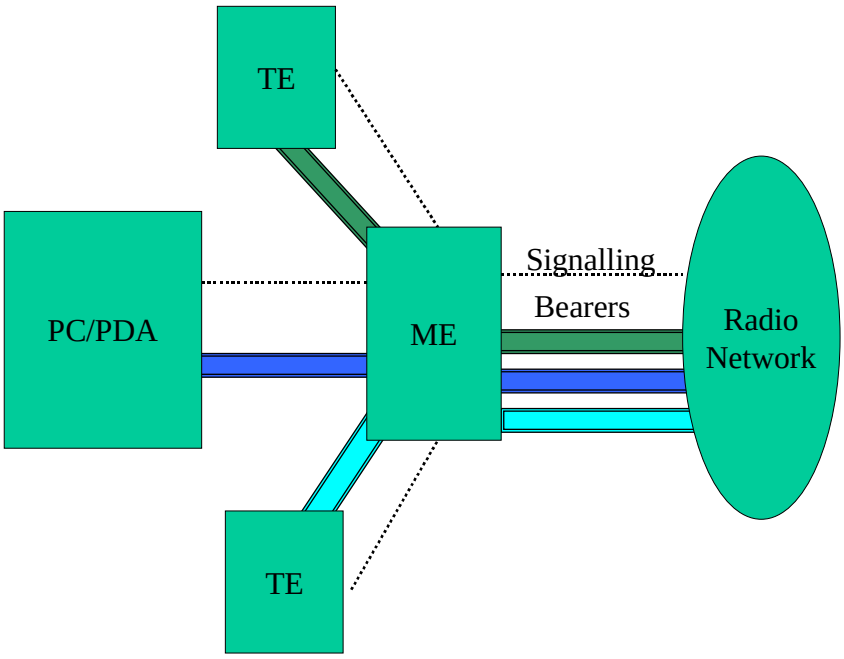
To: TSG-SA

Source: TSG-T

Title:

In the All-IP network, the UE will be required to set up multiple connections with different QoS requirements for different data streams (e.g. signalling, traffic bearers etc.). The issues described in this paper apply to scenarios outside of "All-IP", however it is the "All-IP" network which has caused some discussion in TSG-T.

TSG-T is concerned that the overall framework development has not so far included analysis of the potential for split of functions between the different components of the UE.



The above diagram illustrates an ME connected to a radio network with different TE devices requiring different bearer and signalling capabilities from the ME.

Some questions in this area, which illustrate the problem space are:

1. Is it permitted to use the ME simply as a bitpipe and have an external TE (e.g. PC software) be in control of set up, clear down and manipulation of speech and multimedia calls?

2. What are the user requirements where the UE functions are divided between ME and TE, and which scenarios are required to be supported?

3. How do we maintain security of the network and guarantee proper functionality, if we transfer all the call control functionality out of the ME and into a device whose software can easily be manipulated? How do we avoid denial of service attacks or other security attacks eg. by computing devices (possibly controlled by viruses) instructing the ME to make repeated call attempts into the radio network?

4. What happens to the certification and compliance schemes for the ME if the call control in the ME can be completely bypassed?

In order for TSG-T to understand the problem space with respect to the terminal, and understand the requirements for work items (if any) in this area it is necessary for the required service scenarios and framework to be established by TSG-SA.

It is understood that S4 is already investigating the split of multimedia calling in Release 99 to include a model where all call control is handled by an external TE (e.g. PC) so this could be also relevant to Release 99 scenarios where we have Circuit Switched Multimedia calls.

SA is invited to discuss and consider a work plan to further develop the scenarios which we want to support. In addition to the service scenarios mentioned above it is believed that amongst others this will require discussions on architecture and security aspects in the relevant working groups.