3GPP TSG-T (Terminals) Meeting #12
Stockholm, Sweden, 13 - 15 June, 2001

Tdoc TP-010089

3GPP TSG-T2 #13
Busan, KOREA
14-18 May 2001

T2-010568

Liaison Statement

From: T2

To: T3

Cc: S1, T

Subject: **TS 23.227 v4.0.0 "Application and User interaction in the UE - Principles and specific requirements"**

Contact: Gunilla Bratt (gunilla.bratt@ecs.ericsson.se, +46 70 5693729)

T2 thanks T3 for their review of TS 23.227 presented in T2-010343 (T3-010388) and will below clarify the issues raised.

As a general background, T2 would like to point out that the principles stated in TS 23.227 have been discussed within the community for several years. At the SMG#27 plenary in Prague in October 1998 it was decided to form an SMG level ad hoc group to investigate the issue of conflicts in the UE as relates to resource handling, priorities and the user's needs. This group presented the outcome of its work at the SMG#28 plenary in March 1999 and the principles of AAE (Applications and Automatic Execution) were fully endorsed. It was also concluded that this endorsement was likely to require changes in some existing specifications.

Following the endorsement, discussions have continued in different fora, moving into 3GPP. T2 can see no change in the validity of this work, and have thus adopted these principles into TS 23.227 as follows: Sections 4.1 to 4.4 are copied with minor re-editing and Annex A contains all of the background discussions.

Below explanations per item as written in the T3 paper.

1. It seems to be the case that there are at least some contradictions with TS 22.038, as was suggested might be the case when the principles were endorsed. The key in the example is the user confirmation, which according to TS 23.227 is required. However, it *need not be explicit but can be implicit* via preference settings. These settings can be valid, e.g., per session or keep their values until the user needs to change them.

2. TS 23.227 does not intend to specify a state machine controlling the behaviour of the UE. The problem is most certainly very complex, and that is also the reason why the focus is on principles governing the solution, while the solution as such is left to the manufacturers. T2 can see no conflict but acknowledges that applications independent of the platform on which they run have the same right to require common resources, subject to the needs of the user as well as the basic functions needed to control the network. In order to make a co-existence possible between different applications it is therefore imperative that a certain set of common rules, and even restrictions, be applied to applications and application environments running on the ME or the UICC.

3. When the Bearer Independent Data Transfer Service was introduced, the text in Section 5.1.1, first drafted by S1, was amended by T2 and then reviewed by T3 as well as S1. It is not the intention that the user should be allowed to block administration of applications fundamental to the security of the network. The observation of T3 is correct, but refers to other applications than the aforementioned. Again this goes back to the original principles, based on the fact that the exact circumstance of the user cannot be known beforehand and thus not

necessary priorities.

4. Presently the study of application interaction and co-ordination is out of scope. Partly this might be covered in the Release 5 work when some aspects of UE functional split will be included.

5. Section 4.4 requires that “the ME shall have the capability to.. ”. This is not equivalent to a requirement that the ME should contain the security application itself. In the normal case it is anticipated that the core security applications reside on the UICC, but it is not excluded that the ME can contain such applications, depending on what purpose the product has. TS 03.48 specifies “Security Mechanisms for the SIM Application Toolkit” and T2 understands restrictions made in the TS to be applicable in that context only.

6. Security is of course terminated where the security application resides. MT, in the text of Section 5.2, refers to the MT as opposed to TE, with the underlying assumption of a UICC embedded in the physical module containing the MT. Security in this context does not refer to, e.g., authentication or encryption towards the network, but the security of links between local, physically separate modules and how the division of UE functionality over these might affect e.g., the overall security of the network.

T2 anticipates that TS 23.227 will continue to be improved as well as extended during the Release 5 work, and looks forward to a dialogue with T3 in these matters. During that process other groups like SA1 might also need to be involved in order to achieve a common understanding within 3GPP of these fundamental principles and concepts.