

3GPP TSG SA WG3 Security — S3#17

S3-010016

27 February - 02 March, 2001

Gothenburg, Sweden

TSG-SA WG2
SA2#16 22-26 January 2001
Los Angeles, CA

S2-010392

Liaison Statement

From: TSG-SA2

To: TSG-T2, TSG-SA1, TSG-SA3

Cc: TSG-SA, TSG-T, TSG-T3, TSG-CN1

Subject: **Response to LS (T2-000793) on discussion document on UE functionality split over physical devices**

Contact: DeWayne Sennett
dewayne.sennett@attws.com
+1 425 580 6847

SA2 has reviewed the discussion document on the UE functionality split over physical devices that was provided in LS T2-000793. SA2 has the following general comments:

1. Some of the example scenarios in this discussion document do have architectural impacts. However, since there are no user or system requirements specified, SA2 is unable to determine the scope and magnitude of these architectural impacts.
2. With the information that is provided in the discussion document, SA2 is unable to determine what other related scenarios may have also an architectural impacts.
3. The discussion paper from T2 proposes a security study on the items and scenarios identified in the discussion document. SA2 believes that while a security study by SA3 is required, such a study is too narrow in scope and focus. A feasibility study by SA2 on the architectural aspects would also be required.

Therefore, based upon the above comments, SA2 proposes that SA1 first define the set of requirements associated with items and scenarios of the discussion paper from T2.

Liaison Statement

From: TSG-T2
To: SA3, TSG-T, T3, CN1
Cc: TSG-SA, SA1, SA2

Subject: Discussion document on UE functionality split over physical devices

Contact: Kevin Holley (kevin.holley@bt.com)
Rob Lockhart (rob.lockhart@motorola.com) (+1.561.739.2650) – Annex 1 only

TSG-T2 has continued its discussions on the issues raised in **SP-000353** on the distribution of call control applications in external devices and in **SP-000313** (TP-000115) on Requirements and Scenarios for Call Handling.

In **Annex 1** an example of a use case is presented, which in itself illustrates quite a few problem areas. This is not a unique use case but it is typical of the type of use cases that outside standard development organisations show. We found quite a few problem areas in this one. How many other problem areas would we find if we looked at more?

In **Annex 2** some principal models on the UE functionality split over physical devices are given to provide a starting point for explicit requirements on the relevant interfaces.

TSG-T2 would be happy to consider additional items not included in the annexes as well as scenarios leading to additional principal models and items. Based on work in other industry fora, including USB IF, Bluetooth SIG and IrDA it would appear that at least the models in Annex 2 are envisioned.

It is believed that several cases, including local Piconets as well as extensions of previously identified cases, need an examination by several working groups to reach a common 3GPP position. In trying to solve the problems highlighted in the use case, and considering the models on their own it might be considered to transfer USIM information, or even the proprietary authentication algorithm, over some of the local links. Also, an attempt might be made to solve other problems by implementing L3 call handling in a TE, and the issue is how to verify and guarantee proper L3 operation and how to prevent malicious tampering.

T2 believes that a security study on these and other items is necessary before anyone starts to consider implementing this kind of approach; **a number of principal models should be identified and analysed, thereby specifying what is allowed and what is not allowed in terms of functionality split and local link data transfer.**

Based on the scenarios in these annexes TSG-T2 would like to ask the other groups to provide their understanding of the problems and suggestions for a way forward.

While the other groups might have to amend their specifications to cater for the new cases identified as conclusions of this discussion, it is the intention of TSG-T2 to incorporate the conclusions relevant to them in their specification on the Terminal Local Model (draft TS 23.227, T2-000546).

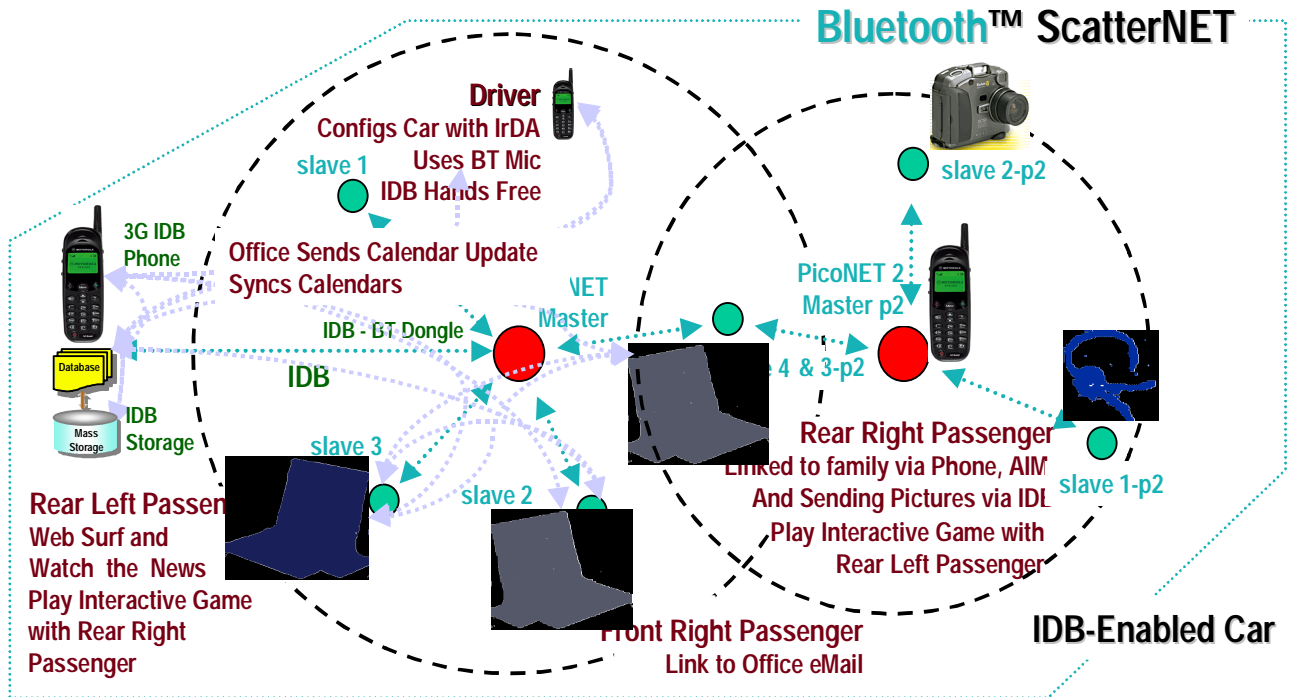
ANNEX 1: A Use Case Example – The Car Pool

The Use Case: Car Pooling in the Wireless Lane

The included animated PowerPoint slide describes a car pool scenario where both the car and its occupants have Bluetooth-enabled communications, computing, and other devices.

1. The scenario starts with a car equipped with both an Intelligent Transportation System Data Bus (IDB) that includes a Bluetooth interface dongle and an Infrared Data Association (IrDA) infrared locking and control port.
2. The car's owner approaches and uses his IrDA-equipped 3GPP mobile phone to unlock and transfer configuration information to the car through the car's external IrDA locking and control port. This configuration information transfer enables the car's IDB-linked 3GPP hardwired mobile phone and, in the process, disables the owner's personal 3GPP mobile phone.
3. The owner's in-progress wide area conversation on the personal mobile phone is transferred to the IDB-connected 3GPP phone via the car's Bluetooth Piconet without dropping the call. The audio path may be through the car's IDB-linked stereo system or through the owner's Bluetooth-linked wireless headset.
4. The owner drives the car to the first car pool pickup point and the first passenger gets into the car.
5. The first passenger decides to pick up her email and turns on her laptop. The laptop discovers the Bluetooth master dongle and existing piconet and proceeds to make a connection to the office email system via the Bluetooth path to the IDB-linked 3GPP phone. Two independent 3G paths through the network are now in process: a voice one from the owner/driver and a data one from the first passenger to the office email system using the office's VPN network on top of the owner/driver's ISP packet connection.
6. The owner/driver then proceeds to the pickup point for the second passenger.
7. The second passenger decides to surf the web and watch the news in Real Video® so he turns on his laptop. The laptop discovers the Bluetooth master dongle and existing piconet and proceeds to make a connection to the internet via the Bluetooth path to the IDB-linked 3GPP phone. Four independent 3G paths through the network are now in progress: a data one from the second passenger to the web and to the second passenger's pay-per-view news service have been added.
8. The owner/driver now picks up the third passenger. The third passenger already has a personal Piconet formed between his Bluetooth-enabled digital camera, his Bluetooth-enabled 3G mobile phone, and his Bluetooth-enabled wireless headset and is sending pictures to his personal web site whilst talking to his wife and sending AOL Instant Messages to his daughter.
9. When the last passenger enters the car, the web surfing passenger decides to play games with the last passenger so the last passenger turns on his laptop. The laptop discovers the Bluetooth master dongle and existing car-based piconet and proceeds to make a connection to the web surfing passenger via the Bluetooth path between them. This laptop also discovers the personal Piconet and proceeds to link the two Piconets forming a Scatternet. The newly available 3G mobile phone is then used to load-share the bandwidth needed by the existing transactions with appropriate billing and packet routing.
10. The office sees that the four car poolers are on line and proceeds to sync up the calendars of the four and download assignment updates during their travel to work. Eleven independent 3G paths through the network are now in progress and load-shared across both available phones: a voice one from the last passenger, a data one from the last passenger to his web site, a data one from the last passenger to his AIM-linked daughter, and four independent data synchronisation operations have been added.
11. The car arrives at work. The owner/driver de-configures the car and in the process transfers his identity back to his personal mobile phone along with the in-progress conversation. The last passenger likewise splits off his conversation from the pooled resources. All four head off to their separate offices.

Car Pooling in the Wireless Lane



DOUBLE CLICK THE GRAPHIC ABOVE TO BRING UP THE ANIMATED PPT PRESENTATION.

Issues raised

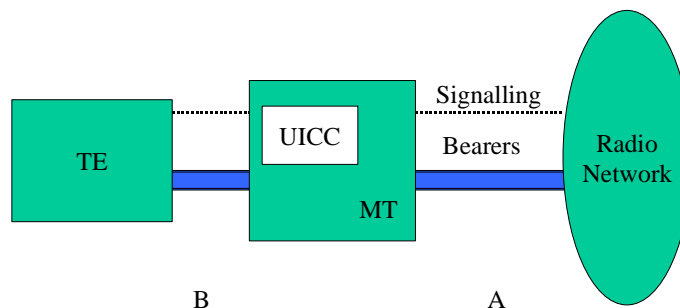
The example above can be mapped to the models of Annex 2.

ANNEX 2: Principal Models on UE Functionality Split

Amongst identified issues illustrated by the models in this annex we find:

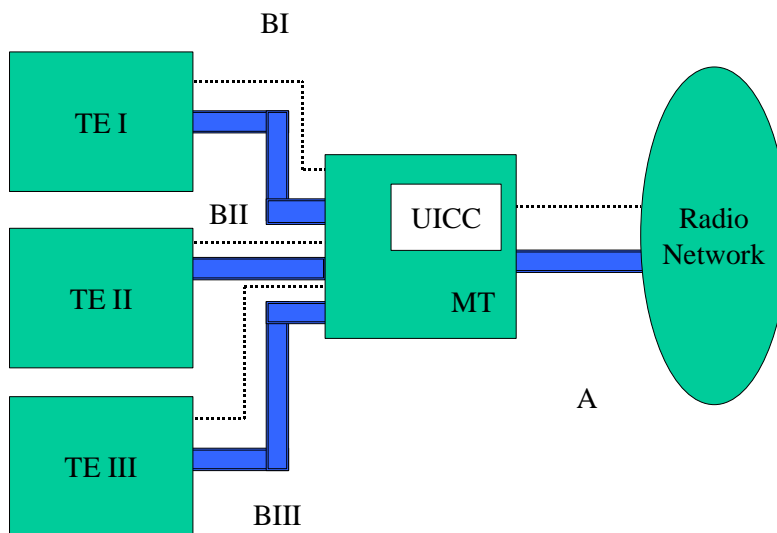
- Encryption - over the local link; from the TE over the radio IF
- Authentication - over the local link; from the TE over the radio IF;
 - PIN handling over the local link
- USIM personal(isation) data - what is allowed to be transferred where and with what requirements on security
 - maintaining the call during this transfer
- USIM security data - what is allowed to be transferred where and with what requirements on security;
 - residence and transfer of operators' proprietary authentication algorithms
- L3 call handling in the TE, transparent to the MT
- Scenarios with call handling in the TE as well as handling of retransmissions
- Charging - when several users utilise the same MT
- Load sharing – per packet between multiple MTs
- Routing – per packet to multiple TEs
- Location of MExE functionality
- QoS aspects on the MT-TE IF in terms of real time response
- Local links issues

Model I:



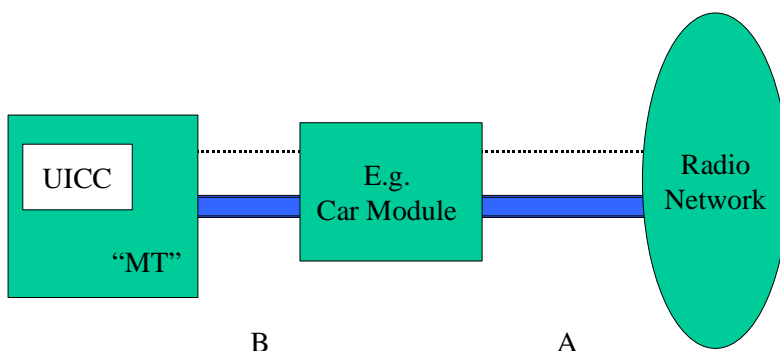
This model corresponds to the present model assumption. A is the ordinary radio interface. B is a cable or a short-range wireless connection. A specific distribution of functionality is defined by GSM 04.34, but recent discussions have challenged that distribution raising a possible move of MT functions to the TE. Other aspects that need looking into are such things as QoS requirements on the MT-TE IF (where the TE does not guarantee real time response) and the location of MExE in the TE. Model II:

This model is based on Model I but uses a piconet locally to allow multiple TEs to connect to the same MT. A possible use case is one user per TE that would request services that require independent charging in spite of accessing the network via the same MT.



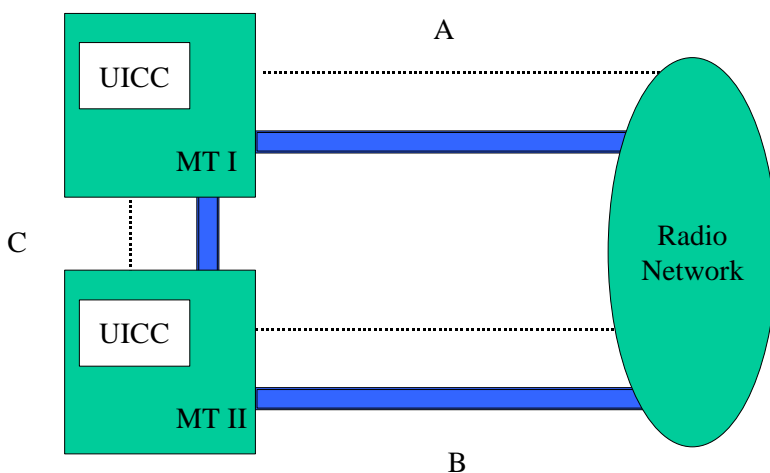
Model III:

Model III is illustrated by the use case in Annex 1, where the user would like to continue her call, e.g., via the pre-installed car equipment after transferring the call from the personal handset. The Car Module can be a specialised module or a “standard” MT module that is connected to handsfree equipment, external antenna, etc. At handover of the call, personalisation data would be transferred to the car. If complete control is transferred to the Car Module, USIM security information is transferred as well. Link B can be a short-range wireless link.



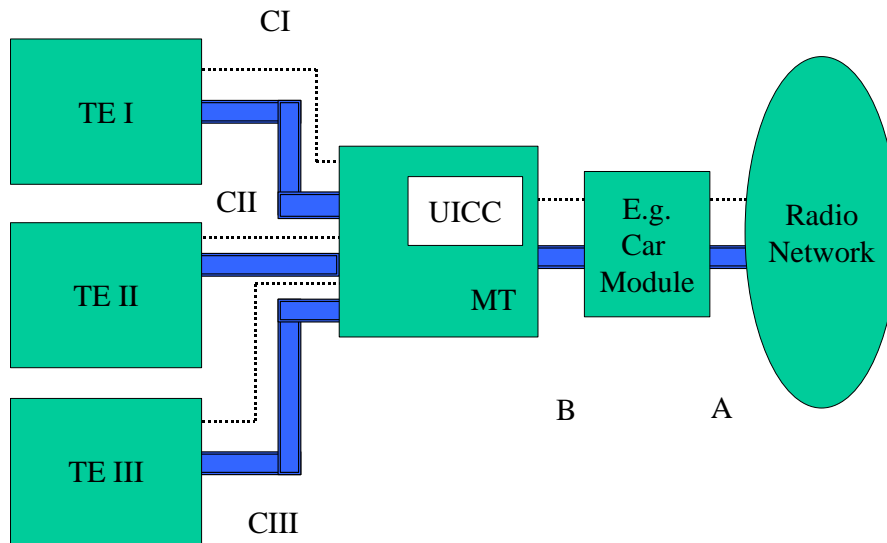
Model IV:

This model resembles Model III for the user, but is significantly different in implementation since separate UICCs are assumed. MT II would, in the case of Annex 1, be incorporated into the Car Module. This scenario requires the two UICCs to co-exist; in the example, UICC I hands over the call to UICC II. Another scenario is the two MTs loadshare the traffic on a per packet basis with significant routing and charging issues. The MTs become, in effect, routers. Link C can be considered to be the same as link B in Model III.



Model V:

Model V combines Models II and III, with all the issues associated with both.



Model VI:

This model shows a piconet where the applications in the TEs interact with or are controlled by applications on the UICC. This corresponds to the Local Link work item in TSG-T3. The link B can be a short range wireless link. This model can, as one might expect, be combined with the other models.

