3GPP TSG SA WG3 Security — S3#18 **S3-010175**

21 - 24 May, 2001

Phoenix, USA

Source: Orange

Title: UE Split over several Devices

Document For Discussion at SA3#18

Adgenda Item: tbd

Introduction

There have been a number of LS and Papers discussing the case of establishing connections through a UE that consists of several separated components, connected by bluetooth, Infra Red, Cable, ore other technology. Here I present a few ideas for the establishment of a security structure for this type of connection.

References

23.227 V1.0.0 Application and User Interaction in the UE - Principles and Specific Requirements

T2-000793 Discussion document on UE functionality split over physical devices

S1-010166 LS from S1 to SA2, SA3, T2, TSG-T, T3, CN1, SA; Date: 9th February 2001

SP-010177 Response to LS (T2-000793) on discussion document on UE functionality split over physical devices

Principals

The security mechanisms should be as strong as that already established for the single component UE.

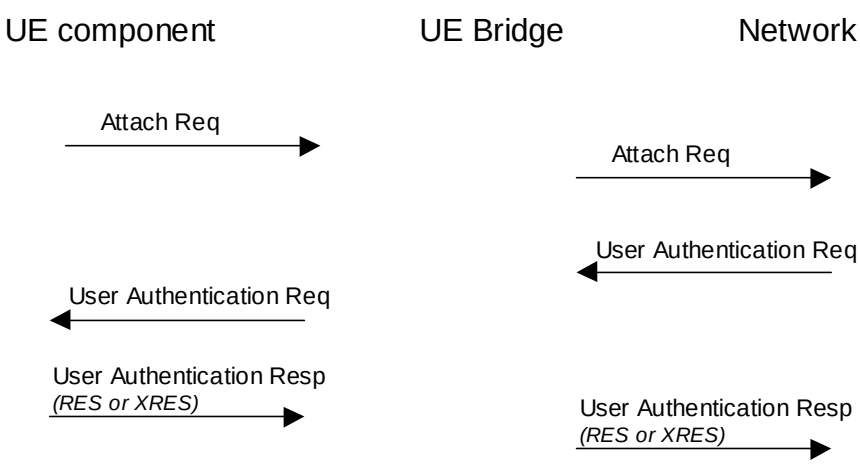
The services used must be clearly attributable to a USIM and associated subscription.

The confidentiality of any inter-linking system will be presumed to be insecure, but it may not be appropriate for us to standardise encryption protocols on these links.

Proposal

Each component should have a SIM or USIM and be capable of performing either GSM authentication or 3GPP AKA

A bridging component (one that is able to connect to a 3GPP network and offering connections to other devices) will allow those devices to attept to connect to the network and will pass GSM or 3GPP AKA message transparently. It will only allow other messages to pass when it has seen a successful AKA sequence pass between the component and the serving network.



Issues

There is no specific response from the network on a authentication success or failure. A success will result in the network responding to the next message. A failure means that the network will ignore further requests from this device. Perhaps an aditional message could be created for this?

Network operators will need to provide customers with additional SIM or USIM cards for these components and link them into the subscription. This may be diffucult as oftern the phone is purchased with the SIM card inserted, and a subscriber may not purchase the other components at the same time or place.

These sort of devices currently do not have USIM / SIM slots incorporated in to them

Current authorisation is implicet, connecting the cable or enabling the IR port is all that is required.

The component's USIM belongs to another network for which the network attached to the UE-Bridge component does not have a roaming agreement. This would most likely arise in a home area with competing networks. Unless the networks agreed to offer roaming agreements then this type of connection woud fail.

Application to the 3 cases listed in S1-010166

The cases outlined were

A) Single user with multiple devices

B) Multiple users with multiple individual devices

C) Multiple users with a combination of individual devices and shared devices

SA1 would like these areas dealt with in order (A=highest priority, C=lowest priority).

This proposal can be applied to all of the above cases with the inclusion in the UE Bridge component of a list of IMSI's that are permitted to use services.

The Attach Request message of an unknown IMSI could trigger a dialogue on this device that would ask for confirmation of the IMSI before further action.

3GPP TS 23.227 V1.0.0 (2001-03)

Technical Specification

3rd Generation Partnership Project; Technical Specification Group Terminals; Application and User Interaction in the UE - Principles and Specific Requirements;

Reference
DTS/TSGT-0223140U

Keywords

3GPP

Postal address

3GPP support office address
650 Route des Lucioles - Sophia Antipolis
Valbonne - FRANCE
Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Internet
http://www.3gpp.org

Contents

Foreword

This Technical Specification has been produced by the 3GPP.

The contents of the present document are subject to continuing work within the TSG and may change following formal TSG approval. Should the TSG modify the contents of this TS, it will be re-released by the TSG with an identifying change of release date and an increase in version number as follows:

Version x.y.z

where:

- x the first digit:
  - 1 presented to TSG for information;
  - 2 presented to TSG for approval;
  - 3 Indicates TSG approved document under change control.
- y the second digit is incremented for all changes of substance, i.e. technical enhancements, corrections, updates, etc.
- z the third digit is incremented when editorial only changes have been incorporated in the specification;

Introduction

The present rapid development of a diversity of new applications and application environments for mobile usage creates a complexity of previously unseen proportions that the Mobile Equipment has to handle.

This specification introduces a generic model approach for the ME environment; the purpose is *not* to categorise the applications / peripherals, but to try to structure the events that are internal and external to, and has to be handled by, the ME Core Functions. This means that the structure or grouping of the events should be made from a *ME centric* perspective. Some applications run on the ME side have counterparts in the network. This specification does not address the functions in the network.

1 Scope

This 3GPP Technical Specification defines the principles for scheduling resources between applications in different application execution environment (e.g. MExE, USAT etc.) and internal and external peripherals (e.g. infra-red, Bluetooth, USIM, radio interface, MMI, memory etc.).

This specification is divided in two parts: Chapter 5 defines a framework for event handling. Chapter 6 addresses some specific issues.

Appendix A contains an informative background to the problem area.

2 References

The following documents contain provisions, which, through reference in this text, constitute provisions of the present document.

- References are either specific (identified by date of publication, edition number, version number, etc.) or non-specific.
- For a specific reference, subsequent revisions do not apply.
- For a non-specific reference, the latest version applies.

[1] 3GPP TR 21.905 3G Vocabulary

[2] 3GPP TS 23.057: " Mobile Station Application Execution Environment (MExE); Functional description; Stage 2".

[3] WAP, WAP Forum, "WAP Technical Specifications Suite", version 1.1, June 1999. (http://www.wapforum.com/)

[4] 3GPP TS 31.101: "3rd Generation Partnership Project (3GPP); UICC / Terminal Interface; Physical and Logical Characteristics".

[5] 3GPP TS 31.102: "3rd Generation Partnership Project (3GPP); Characteristics of the USIM application".

[6] 3GPP TS 31.111: "USIM Application Toolkit (USAT)".

[7] 3GPP TS 22.038: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects ; USIM/SIM Application Toolkit (USAT/SAT); Service description; Stage 1".

3 Definitions and abbreviations

3.1 Definitions

For the purposes of this document the following abbreviations apply in addition to those defined in the referred documents:

call: The term call means voice and data calls, USSD, SMS, fax, GPRS calls, supplementary services, etc.

preferences: includes authorisations, priorities, options, etc.

authorisation: means permission to set up and / or receive any call or only certain types of call and access rights to user data.

ME Core Functions: software functions that contain the central logic for the ME, including for instance the scheduling of events.

3.2 Abbreviations

For the purposes of the present document the following abbreviations apply:

MExE: *Mobile Execution Environment*

MM: *Mobility Management*

RR: *Radio Resource*

USAT: *USIM Application Toolkit*

WAP: *Wireless Application Protocol*

5 Principles for the Framework

The model presented in appendix A defines a framework specifying *principles* for event handling, with the focus on issues related to application interaction. Principles for the framework are given below, using the stated definitions. The list is not necessarily complete.

5.1 Basic principles

1. Irrespective of the principles given below, emergency calls shall override all other calls.
2. The ME is the central resource and schedules internal and external entities according to the user's preferences and external environment .

5.2 User requirements

1. The user shall have the capability to make the ultimate decisions as elaborated below. Additionally, in the case where an UE is unmanned, none of the issues below shall render the UE inoperable such that it requires manual intervention locally at the UE to restore its use.
2. The user shall have the capability of selecting preferences interactively and / or via prior set-up in one or more user profiles. These shall be valid on a global or on a per application basis. The user's preferences shall be retained even in the event of loss of power.
   Preferences can be selected for an application when it is installed, or at any other time thereafter.
   Preferences, notably but not exclusively the priorities, can be modified at any time and this shall have effect at the earliest possible opportunity thereafter.
3. The user shall have the capability to modify authorisations assigned to applications. These shall be valid on a global or on a per application basis in one or more user profiles.
4. The user shall have the option to be advised to what extent an application has been authenticated at installation-time, and prevent the application from being installed based on this advice.
   The user shall have the option to be advised about the integrity of an application at installation-time, and prevent the application from being installed based on this advice.
5. The user shall have the capability to abort or suspend any on-going call that has been set up automatically by an application.
6. The user shall have the capability to require that the ME request permission from the user for individual calls, sets of calls (for instance all calls by a certain application) or all calls. The user shall have the capability to request the ME to record information on individual calls, sets of calls or all calls.

7. The user shall have the capability to distinguish which entity / application caused a specific event. The ME uses this information to support the user's preferences. The ME shall be able to inform the network of entity / application at set up time to support trace-ability when a call is set up.
8. The user's privacy shall be protected. Access to user data (including user profiles and any personal information in the UE) and audio functions (this would prevent for instance a mechanism that allows eavesdropping) shall not be possible without the user's prior permission.
9. The user shall have the capability to request from the ME which applications are present in the MExE environment and the (U)SIM, and whether they are running. The user shall also have the capability to request from the ME the status of other interfaces as shown in Figure 1, where implemented.

5.3 Additional requirements on applications

1. An application shall not assume that it is the only one active. For example where several applications use the same interface the application and / or the protocols used over the interface must be able to handle contention.
2. An application shall not interfere (terminate, suspend or degrade) with on-going calls set up by another application without authorisation from the user. For certain combinations of call (e.g., voice/data and USSD messages), interference can happen resulting in a level of degradation.
3. An application shall not assume that it has priority over another application, and shall comply with the user's currently selected preferences.

5.4 Additional requirements on the ME

1. The ME shall have the capability to authenticate the source of the application.
2. The ME shall have the capability to assure the integrity of an application.

6 Specific Interaction Requirements

The following sections detail specific interaction requirements

6.1 Bearer Independent Data Transfer

Bearer Independent Data Transfer is a USIM feature that allows the USIM to request the ME to set up and manage a data channel (using a CSD, GPRS, SMS or USSD bearer) using information provided by the USIM. Once the call is established, data may be transferred through that data call. The details for the USIM/ME interface are specified in TS 31.101, 31.102, and 31.111. The Service Requirements for this are specified in TS 22.038.

6.1.1 Interaction between Core ME functions and Bearer Independent Data Transfer Service

When a Bearer Independent Data Transfer Service is requested by the USIM, the ME shall:

- If the ME is idle, set up the data channel as requested, indicating to the user by appropriate means, e.g., with an icon, that one or more calls are in progress and confirming to the USIM.
- If the ME is not idle and can not service the request without negative impact on ongoing services, then the ME shall indicate to the USIM that the data channel can not be set up. However, if the user has indicated a preference for servicing such requests despite the negative impact then the ME may proceed as in the bullet point above.
- If the user requests that the call be terminated via MMI or other interface, then the call shall be terminated and the USIM shall be informed.
- If an external device (TE, Bluetooth device etc.) requests the same resource then that request shall be denied.

The above behaviour may be modified by a change of user preferences, for example the user may request the ME to deny access by the USIM to a data channel, or the user may request the ME to prioritise a particular external device such that a call set up by a USIM is cleared in order for the external device to be able to make a call.

6.2 Services and applications external to the MT

In the tele- and datacom community there exist today use cases for moving internal interfaces out of the MT; they are required to fulfil user expectations of what services and features 3G MTs should offer.

However, discussions on security clearly show that services should be terminated in the MT, while applications can, as today, terminate in the TE. A possible UE functionality split should not allow internal interfaces (including USIM) to be moved to external interfaces, neither using USAT local link nor other interfaces.

This is a precaution that shall be taken until suitable procedures against misuse have been found and standardised.

Annex A (informative): Interaction handling

In this specification we illustrate possible types of interaction handling for a ME that already can be required or that currently are being developed in standards and industry fora. Although it is probable that only a subset of these entities will exist at the same time, there is no way of knowing the particular combination of applications or a particular users needs relative to this in advance; ***a general way to handle the co-existence must still be defined***.

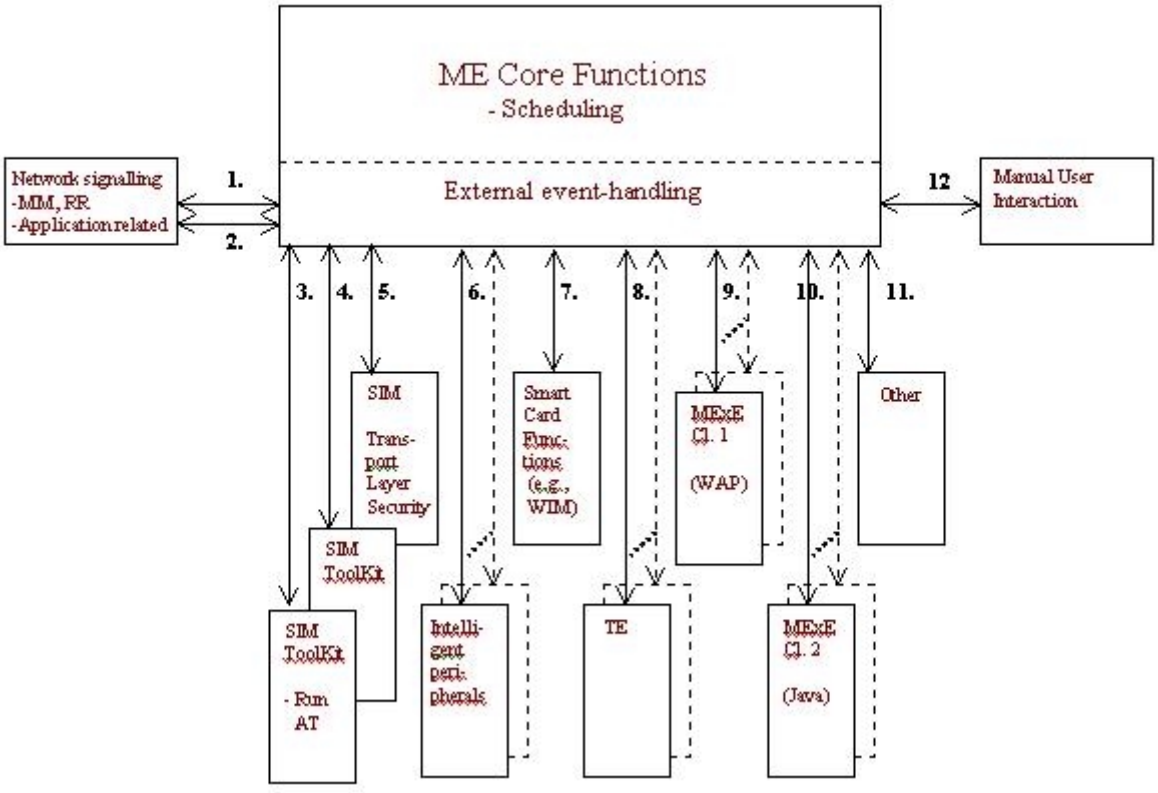
A framework, defining general rules for handling this co-existence of several external functions is outlined in this document. The framework states requirements for the behaviour of the external functions as well as principles for the co-existence as such. As an example, several of the external functions below, or protocols used by them (e.g., the AT-commands) assume a one-to-one relation between them and the ME Core Functions, implying a lack of specified mechanisms to handle a multitask environment.

A.1 The model approach

The model below proposes a *conceptual* split, meaning that the entities and their interfaces are *logical* and need not correspond to any physical division. Before the figure is presented some clarifications and general comments are needed:

- The *ME Core Functions* should be understood as the (collection of) software functions that contain the central logic for the ME, including for instance the scheduling of events.
- With *external event* is meant interaction that an application / peripheral wants (requests / commands), as well as necessary handling of network signalling, user request via the keys, etc. External does not imply whether an external interface is used or not.
- Some *network signalling* is easy to refer to basic network functions, such as Location Update, while other signalling has been invoked by an application.
- The user can interact / intervene *directly* via keys, etc. This is indicated with the *Manual User Interaction* entity. The user can of course do the same via, e.g., a PC or a MExE application, but the events that such actions create is here viewed like the other events that these entities can create.
- The *USIM* / general *Smart Card Functions* are split into several logical entities: the Transport Layer Security, meaning “basic” 2G/3G security; the USIM Application Toolkit; USIM Application Toolkit Run AT-command; and other functions, such as the WIM, the WAP Identity Module, that is being specified.
- The *TE*, Terminal Equipment, is a PC or another piece of equipment that can run applications independently.
- An *Intelligent Peripheral* could be an advanced charger or a car hands-free installation.
- The *MExE* entities are as defined in [2].
- *Other* includes ME resident applications and allows for future applications, and, if that is needed for the model, could correspond to other external devices such as a microphone.

- The interfaces as shown in the figure are logical. In practice the applications run in the ME, a TA or on its own separate platform, and the interfaces are then ME internal or external via a physical connector, IrDA, or Bluetooth.



The figure shows the extent of the complexity that the ME will be expected to handle. It is obvious that a generic framework for conflicts, error handling and interactions is needed. In particular, the following issues can be noted:

1. Priorities of the event handling – the ME does the scheduling and this should be according to the user's preferences.
2. User control – the user's wanted / required interaction; his/her knowledge and control of the events; user integrity for instance for personal data, the ME position, etc.
3. Trace-ability – which entity / application has caused a particular event. This information is required input to solve several of the other issues.
4. Consistency - in the actions of the ME Core Functions relative to the specific application. Several applications and priority levels interact.
5. The validity of commands – for instance call validity when the ME is in the Home PLMN or roaming.
6. Network signalling aspects – how does for instance a dual mode ME treat applications specific to only one of the standards.
7. It might be necessary to look into mechanisms for rejection and termination by the ME Core Function (upon user choice) for applications, calls etc.
8. Testability – the ME manufacturer must be able to as far as possible verify the behaviour of the product, and this should be taken into consideration when the framework is specified. Conformance testing, however, is only relevant to the extent that already is tested.
9. Security aspects – for the protection of the ME and the network mechanisms like authentication of the applications might be required.

Further, the entities have different characteristics; this can possibly be used by the framework definitions. The following can for instance be noted:

1. Several of the entities work together with network nodes, some as slaves (e.g., SIM) and others invoking commands (e.g., WAP). Others, like the intelligent peripherals, only communicate “locally”.
2. The entities can be active or passive. In the latter case the ME has more knowledge about the expected behaviour, since they only execute functions upon request and cannot issue commands independently.
3. Some events refer to “basic” network handling, some to manual user interaction, and others relate to application invoked functions. “Basic” network interaction should then have priority if such a distinction can be made. Consideration should be given to incoming calls.

Annex B (Informative): Change history

Change history		
V 0.0.0	May 2000	
V 0.1.0	August 2000	Clarification of Section 7.
V 0.1.1	February 2001	Restructure of document to clarify normative parts. T2-010281
V 0.1.2	February 2001	More references included, clarifications in basic principles for the framework and move history chapter T2-010289
V 0.1.3	February 2001	Change to agreed tittle in T2#12 closing plenary Updated reference
V 0.2.0	March 2001	- Removed reference about SyncML - Updated references and abbreviations - Added ME Core Functions definition in chapter "3.1 Definitions" - Moved from last 2 sentence from chapter 4 to chapter "1 Scope" - Move chapter "4 Introduction" after "Foreword" - Chapter 5: re-numbered the requirements, starting with 1. in each chapter. - Added chapter "6.2 Services and applications external to the MT"
V 1.0.0	March 2001	Presentation for approval to TSG-T#11

TSG-SA WG 1 (Services) meeting #11
Capetown, SA 6th to 9th February 2001

TSG S1 (01) 007
Agenda Item: 5.3

Technical Specification Group Services and System Aspects
Meeting #10, Bangkok, Tailand, 11-14 December 2000

TSGS#10(00)0632

3GPP TSG-T2 #11
Shin Yokohama, JAPAN
November 27th - December 1st 2000

T2-000793

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.

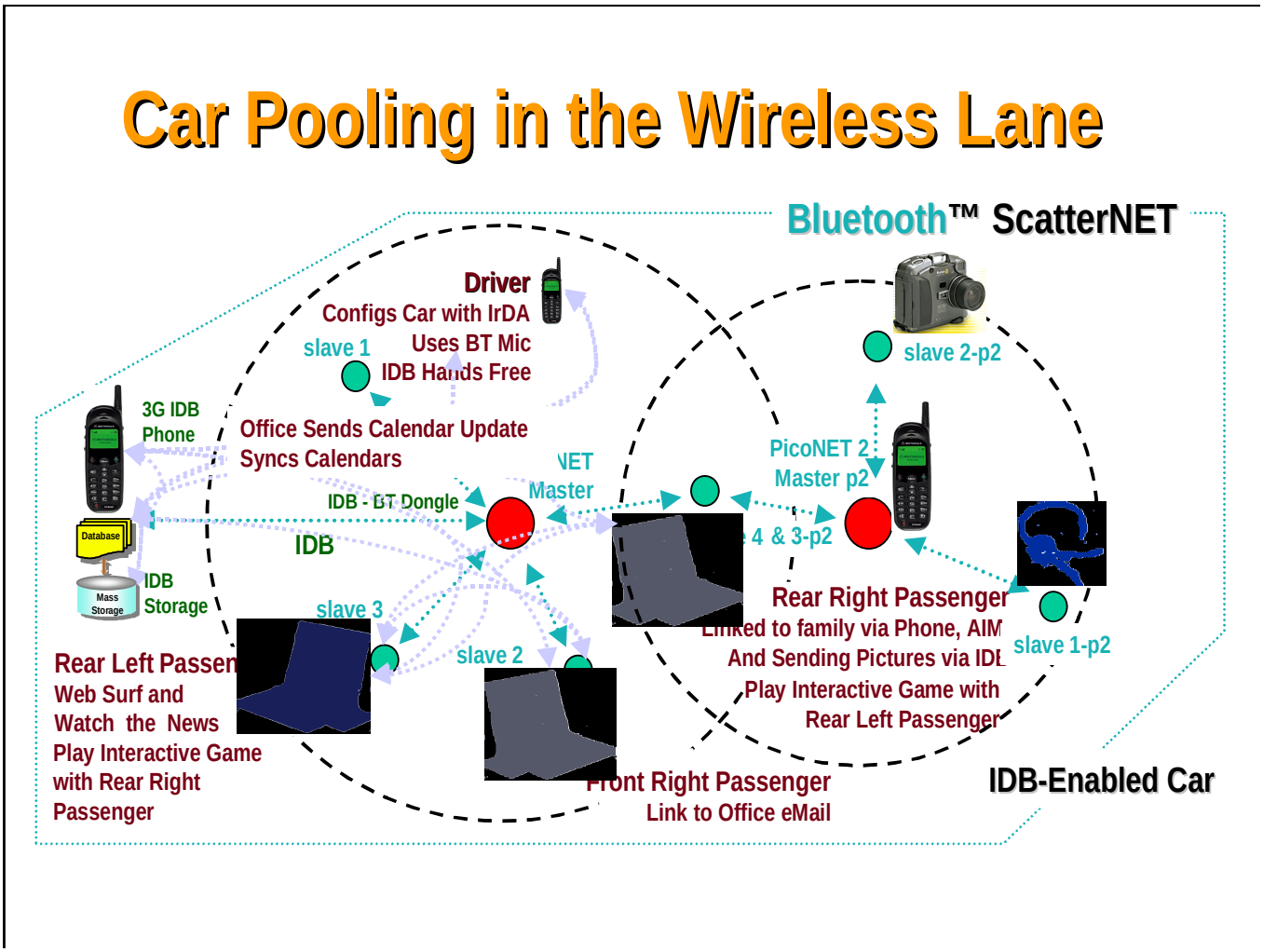
7. The second passenger decides to surf the web and watch the news in Real Video® so he turns on his laptop. The laptop discovers the Bluetooth master dongle and existing piconet and proceeds to make a connection to the internet via the Bluetooth path to the IDB-linked 3GPP phone. Four independent 3G 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 whist 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.



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.

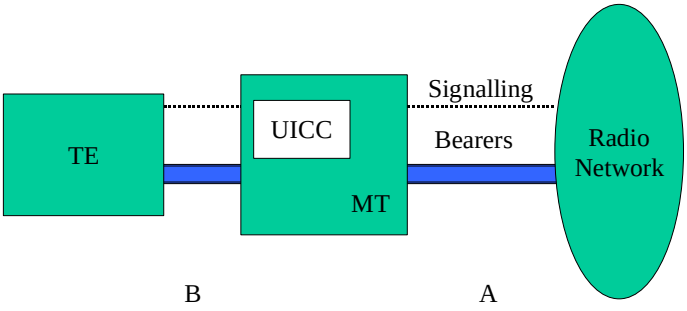
ANNEX 2: Principal Models on UE Functionality Split

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

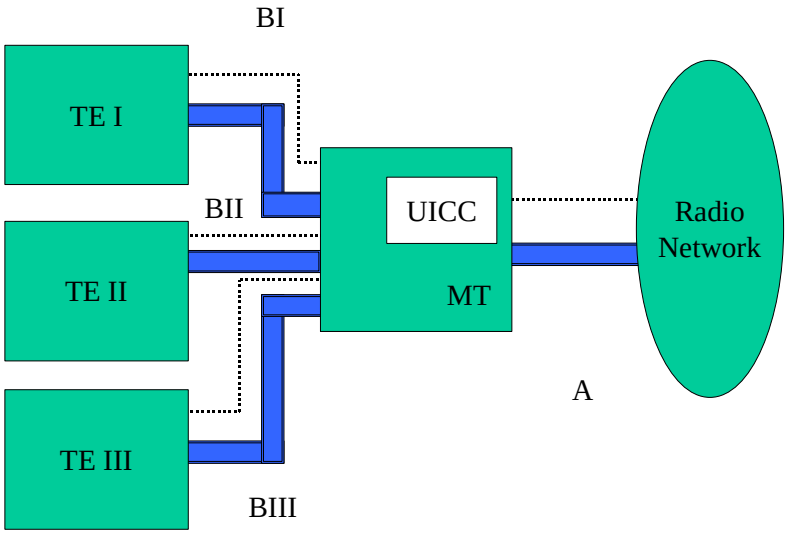
Model I:

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.



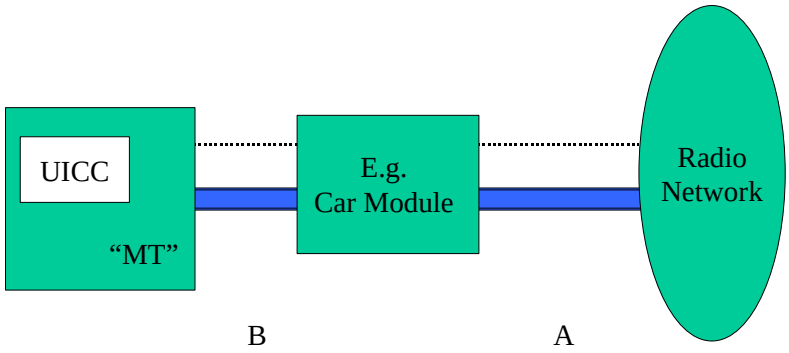
Model II:

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.



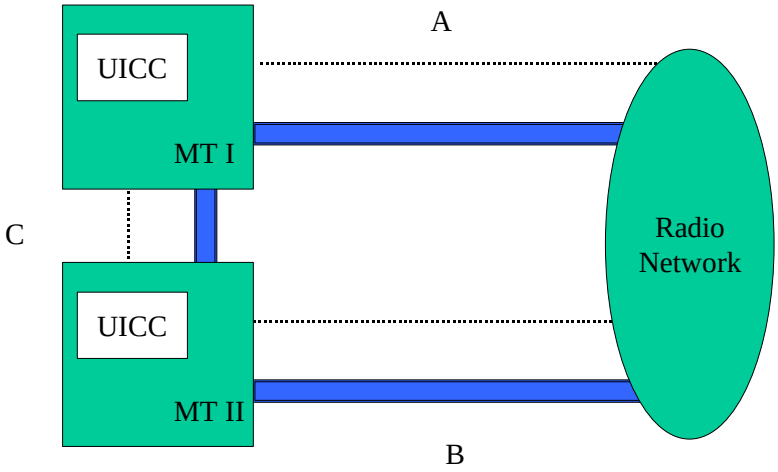
Model III:

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.



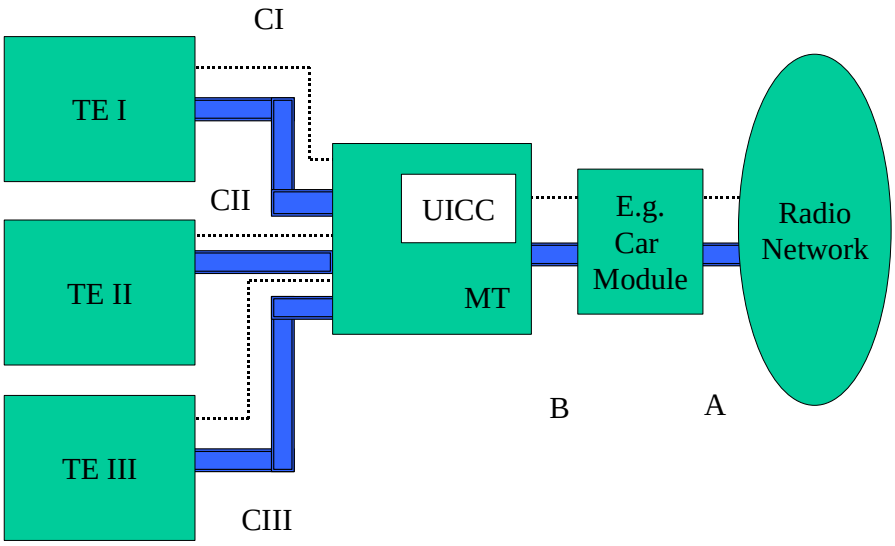
Model IV:

This modelresembles 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.



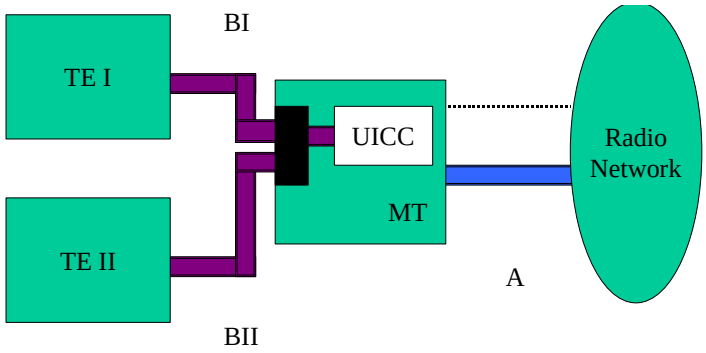
Model V:

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.



TSG-SA WG 1 (Services) meeting #11 *TSG S1 (01) 0166*
Capetown, SA 6th to 9th February 2001

PROPOSED LIAISON STATEMENT

From: **SA1**

To: **SA2, SA3, T2, TSG-T, T3, CN1, SA**

Date: **9th February 2001**

During the 6th Feb a paper from T2 on UE functionality split was presented to SA1 (S1-010007). This paper asked which models should be made available to users in order to satisfy the requirements of the marketplace. The T2 paper outlines an example of car pooling and makes some suggestions about the types of scenario which could be envisaged in terms of split of functionality.

SA1 in general believes that the marketplace will need solutions which allow the maximum flexibility in order to provide innovative services. However SA1 also recognises the requirement for security so that the user is not denied service and service is not stolen from the Home Environment.

SA1 believes that SA3 is in the best position to determine which of the scenarios in Annex 2 can be provided in a secure way, and encourages SA3 to analyse this and provide an answer. SA1 believes that the detailed architectural analysis in SA2 will be helped if the number of scenarios can be reduced and therefore it would be advantageous to know whether some of the scenarios can be discounted from a security point of view first.

SA1 also believes that the problem of sharing UE functionality and resources should be divided into three areas:

A) Single user with multiple devices
B) Multiple users with multiple individual devices
C) Multiple users with a combination of individual devices and shared devices

SA1 would like these areas dealt with in order (A=highest priority, C=lowest priority).

For example, from the SA1 perspective, it is unclear that the "Car Pooling" scenario in Annex 1 is particularly realistic, and while it seems sensible to analyse some simple requirements, like a user getting into a car and having service inside and outside of the car environment, the kind of requirement like sharing bandwidth between different people in the same car is very advanced and should be a much lower priority.

In the scenario in Annex 1, SA1 would like to have the ability to handover an existing call from the external environment to the car environment, and also the ability to have service inside a car environment where that car is a rental car and previously "unknown" to the user getting into the car. SA1 would like comments on the feasibility of introduction of these features.

This is only an initial analysis and SA1 will look further into this in future meetings, as well as analysing SA1 specifications for appropriate changes.

SA1 looks forward to future co-operation with other WGs.

Technical Specification Group Services and System Aspects
Meeting #11, Palm Springs, USA, March 2001

TSGS#11(01)177

Source: **T3**

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

Document for:

Agenda Item:

3GPP TSG-T (Terminals) Meeting #11
Palm Springs, USA, 14 - 16 March, 2001

Tdoc TP-010066

3GPP T3 Meeting #18
Sophia Antipolis, France, 1 - 2 March, 2001

Tdoc T3-010250

Liaison Statement

From: T3

To: T2, SA3, T, CN1

Cc: SA, SA1, SA2

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

Contact: Ileana Leuca (ileana.leuca@attws.com) +1 425 580 7900
Sonia Compans (sonia.compans@gemplus.com) +33 4 42 36 44 47

On 22-23 of February, a joint ad-hoc meeting between TSG-T2 and TSG-T3 addressed the UE functionality split over physical devices, a subject raised in T2-000793. The group has analysed a draft document outlining different cases in a "car pooling" scenario. T3 is glad to share the group's current understanding on this matter.

The analysis was USIM/UICC centric and based on the following considerations:

- A UICC/USIM is required to access the 3G network.
- Charging is linked to one particular USIM.
- The secret key and the authentication algorithm cannot be transferred out from the UICC.
- A periodic UICC presence detection is mandatory during a call.

The group decided to assemble a set of cases based on a generic issue such as billing associated with different subscriptions, when a user(s) uses one or multiple devices.

Based on the fact that the subscription information is stored in a USIM and that the USIM application resides on a UICC, four cases were identified (see Annex 1).

This is only an initial analysis. T3 believes that a security study and a feasibility study on the architectural aspects of these USIM/UICC models should define a minimum number of models by eliminating the ones violating the 3G security and architecture requirements.

Should other groups have to amend the set of cases, based on other factors, TSG-T3 will be happy to re-visit this subject.

T3 looks forward to future fruitful co-operation on this topic.

ANNEX 1: A Use Case Example – The Car Pool

Case 1

In this case, multiple users, (e.g. one, two or three) use one subscription and its information is stored in one USIM/UICC as shown in Fig. 1. For the car pool scenario, the car module has its own UICC with one USIM and all the passengers use this subscription. The user(s) identity is different from the subscribers' identity.

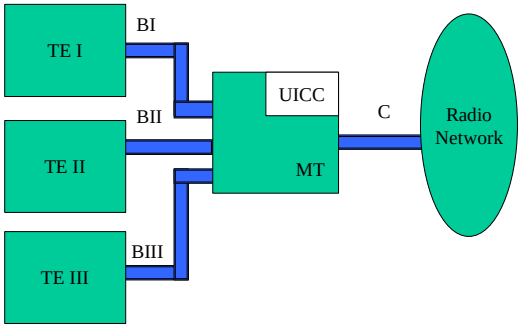


Figure 1 – Multiple users, one "borrowed" subscriber identity.

Multiple independent 3G paths through the network are required.

Case 2

In this case, multiple users use multiple subscriptions residing in one UICC. For the car pool scenario, the car module has its own UICC with several USIMs and each user accesses different services using a dedicated USIM (every usage is metered). The billing is associated with the subscriber's identity stored in the USIMs.

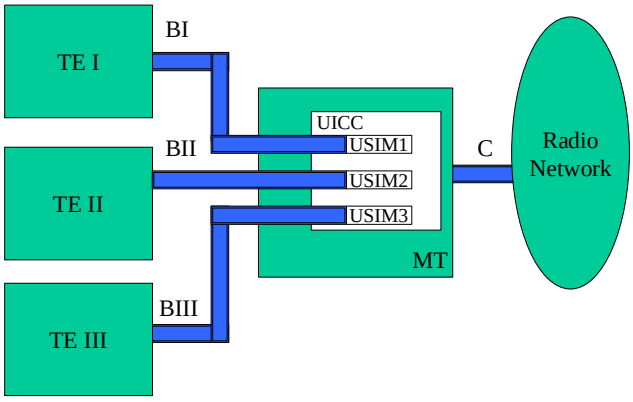


Figure 2 - Multiple users, multiple "borrowed" subscriber identities.

Multiple independent 3G paths through the network are required. In release 99 we may have multiple USIMs stored on a UICC but they cannot be all active at the same time. In release 4, the support of logical channels enables multiple USIM activation. However, further studies are needed on the terminal and network sides regarding the support of multiple active USIM calls/sessions simultaneously.

Case 3

In this case, every user uses subscription per device and each device (e.g. PC, PDA) has an UICC/USIM. For the car pool scenario, the car module does not use an USIM/UICC, even if an USIM/UICC is physically present in the car module.

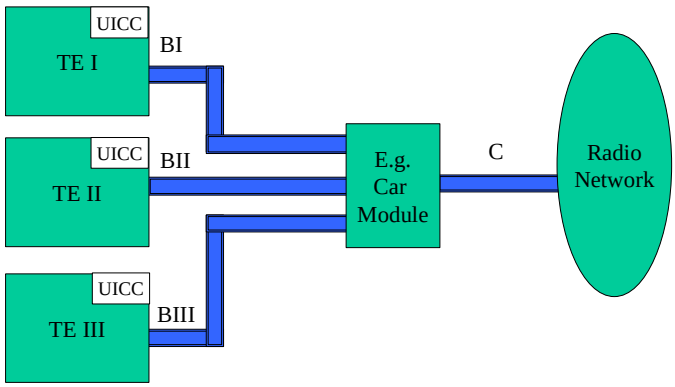


Figure 3 - Multiple users, multiple "owned" subscriber identities.

Two scenarios can occur

a) The car module is used as transmitter with multiplexing capabilities and the CK and the IK are handled by the TEs.
b) The car module also handles the CK and IK keys. The transfer of the CK and IK between the TE and the car module can raise a security issue. As one radio link can only be associated with one valid CK/IK, it is assumed that multiple radio transmitters exist on the car module.

This scenario requires each device accessing the 3G network to have a 3G USIM/UICC.

Case 4

In this scenario, every user has a subscription i.e. each user has one UICC/USIM that resides in a device such as the mobile phone (like in case 3). However, when the user becomes a passenger, in a car pool environment, two approaches are considered:

a) The user stops using the UICC of his device and the device notifies the network that from now on, it will use the car module USIM/UICC, as in case 2 (figure 4).
b) "Mobile hand-over": the user continues using the initial UICC and the radio transmitter of the car module (figure 4). This case can also evolve into having a second TE using the UICC from the ME and using the radio transmitter from the car module (figure 5).

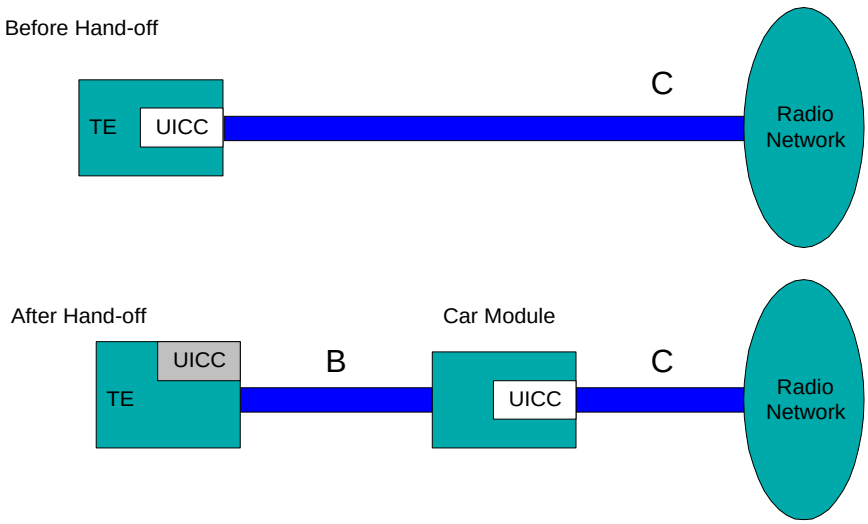


Figure 4 - Hand-off to a "borrowed" subscriber identity.

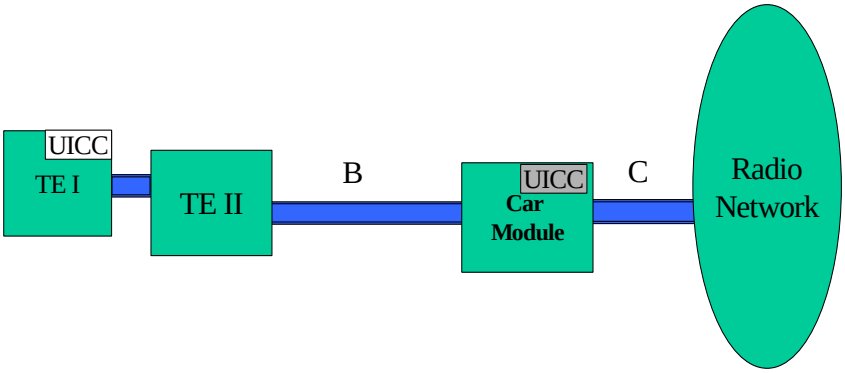


Figure 5 – Hand-off, but retain and lend "own" subscriber identity.

In the "mobile hand-over" case, the TE transmits the messages, including the CK and IK keys, received from the UICC to the car module through the local link. The transfer of the CK and IK between the TE and the car module can raise a security issue.