3G TR 22.907 3.1.2 (1999-04)

Technical Report

3rd Generation Partnership Project;
Technical Specification Group Services and System Aspects
Service aspects;
Terminal and smart card concepts
(3G TR 22.907 version 3.1.2)

Reference

DTS/TSGS-0122907U

Keywords

<keyword[, keyword]>

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 Report 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 TR, it will be re-released by the TSG with an identifying change of release date and an increase in version number as follows:

Version 3.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;

1 Scope

This document is informative and applicable to standardisation work within ETSI SMG for UMTS. It discusses the issues related to terminal and smart card concepts in the UMTS environment. The report will provide guidance and input to the SMG specification work in the area of UMTS terminals and IC cards used for containing UMTS information and accessing UMTS services. It presents various options on the roles relating to IC cards and terminals as well as discussing their relationship in UMTS.

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.
- A non-specific reference to an ETS shall also be taken to refer to later versions published as an EN with the same number.

2.1 Normative references

[1] UMTS 22.01(V3.1.0): “Universal Mobile Telecommunications System (UMTS): Service Aspects;

[2] ISO - 7816-1, 1987: "Identification cards - Integrated circuit(s) cards with contacts, part 1: Physical characteristics";

[3] ISO - 7816-2, 1988: "Identification cards - Integrated circuit(s) cards with contacts, part 2: Dimensions and locations of the contacts";

[4] ISO - 7816-3, 1989: "Identification cards - Integrated circuit(s) cards with contacts, part 3: Electronic signals and transmission protocols";

[5] ISO - 7816-4, 1995: "Identification cards - Integrated circuit(s) cards with contacts, part 4: Inter industry commands for interchange";

2.2 Informative references

[6] ETSI TC SMG PT Mexe, “Mobile Station Execution Environment, Feasibility Study”, 24-25 September 1997;

3 Definitions and abbreviations

3.1 Definitions

For the purposes of the present document, the following definitions apply:

USIM: User Service Identity Module is an application residing on the IC Card used for accessing UMTS services of a certain Service Provider.

3.2 Abbreviations

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

ADN	Abbreviated Dialling Numbers
API	Application Programming Interface
CPU	Central Processing Unit
GSM	Global System for Mobile Communications
IC	Integrated Circuit
JPEG	Joint Photographic Experts Group
MIPS	Million Instructions Per Second
MMI	Man Machine Interface
NO	Network Operator
PC	Personal Computer
SIM	Subscriber Identity Module
SP	Service Provider
SW	Software
UMTS	Universal Mobile Telecommunications System
USIM	User Service Identity Module
VASP	Value Added Service Provider

4 Introduction

UMTS aims to offer service capabilities that enable a wide variety of services to be implemented. Such services range from simple services like speech, to complex multimedia services containing several simultaneous media components that place totally different requirements on the system and on the terminal equipment. By standardising service capabilities rather than actual services, more flexibility is available for service providers/network operators to create unique services.. The same principle also applies for UMTS terminals, i.e. the types of terminals are not standardised and are therefore not limited in any way. A wide range of terminal types is likely in the UMTS environment, e.g. speech only terminals, videophones, data terminals, wideband data terminals, fax terminals, multi-band/multi-mode terminals and any combination of the aforementioned.

2nd generation digital cellular terminals already contain considerable complexity. There are two main reasons for this. Firstly, cellular systems themselves require a huge amount of functions to be fulfilled, from channel and speech coding to signalling and data protocols. In addition to those functions, all terminals have their own mobile system independent features, sometimes also called as Value Adding features. Examples of these are, memory databases, speech recognition, messaging features, display functions, and different source coding methods (e.g., JPEG).

Terminal development trends for today’s terminals are mainly towards higher integration levels resulting in smaller size. The goal of “four 100’s” has been a rule of thumb target for handsets, i.e., 100 hour standby, 100 cc size, 100 gram weight and also 100 MIPS performance. The size targets have already been achieved and any requirement for smaller terminals is questionable from the usability and physical size limitations perspective. The other target parameters have no maximum limitations. On the other hand, we can see the following further trends for near future terminals:

- Application specific terminals (smart traffic, vending machine radio, etc.);
- Increased number of value adding features (graphics, smart messaging, PC connectivity and compatibility);
- Support for higher number of source codecs (several speech codecs);
- Multiband terminals (e.g., GSM in 900MHz and DCS1800);
- Multimode terminals (e.g., GSM/DECT dualmode terminal);
- Dynamic SW configurability;

These trends are more than likely to continue in the future. Multiband and multimode terminals with high integration levels would be preferred by the users. Technological development of these terminals relies on new packaging and interconnection technologies, as well as technological steps like SW-radio. The concept trends of mobile handheld terminals is likely to diverge from simple speech terminals towards a variety of different types, e.g., communicators, wearable phones, data terminals, etc. The dominant role of speech terminals will be challenged in the future by these new data- and multimedia-oriented terminals.

The UMTS user service identity module (USIM) shall contain sufficient information to identify the user and service provider. USIM is UMTS specific application residing on a IC card and is required for service provision. Authentication and ciphering functionality may be part of USIM or some other application on the same or different IC card. The UMTS IC card could also support applications other than UMTS USIM application in order to allow more versatile UMTS IC card functionality such as access to value-adding services.

The trend for IC Cards is similar to that for terminals. The next generation of IC Cards will be multi-application cards capable of supporting several applications simultaneously. Furthermore, applications could be downloaded to and removed from these cards, both at the time of issuing and during the card’s lifetime The advent of these virtual machine cards, e.g. Java cards and Multos cards, will change the roles of the card issuers and application providers, and will enable IC cards to be much more flexible in the future.

5 Technology development

New radio-interface and system capabilities will enable higher quality multimedia services to be provided and therefore new terminal concepts to evolve. The variety of terminals in the UMTS environment will evidently be large. Terminal implementation technologies, such as digitalisation providing programmability and terminal configurability, VLSI, and display technologies, have developed a lot recently and will undergo further development in the future. Processing power, implementation architectures, IC and passive integration, and memory technologies are developing rapidly and will facilitate an increase in terminal functionality that will enable higher integration of terminals, as well as the integration of more functionality into smaller terminals.

It can be clearly seen that the technical development of IC card technology increases the available possibilities for IC cards in the UMTS context. Compared to current IC cards (e.g. GSM Phase 2 SIM cards), the amount of memory and processing power will increase significantly. These development trends will meet the requirements of UMTS and should be taken into account while defining the features and functions of UMTS IC card.

6 IC Card Functionality

6.1 Mandatory functionality for IC card containing a USIM

The mandatory requirements for IC Cards used for holding USIM application, are related to the need to have one USIM application on the IC card, as well as to the security issues. The following functionality is required from the IC card holding a USIM application:

- Physical characteristics same as used for GSM SIM
- The support of one USIM application
- The support of one or more user profile on the USIM
- Possibility to update USIM specific information over the air, (e.g. such information as service profile information, algorithms, etc.) in a secure and controlled manner.
- Security mechanisms to prevent USIM application specific information from unauthorised access or alteration. Verification of the access privilege shall be performed on the card itself and not delegated to another entity (for example the terminal).
- User authentication.

6.2 Desirable optional functionality for IC card containing a USIM

The standard should support the following additional functionality for the IC Cards in UMTS environment:

- The support for more than one simultaneous application (Multiple USIM, Ecash and/or some other applications).
- Possibility to have shared applications/files between multiple subscriptions, including ADNs, other user/SP controlled files and data, as well as for as yet undefined applications (including downloadable applications) required by future services. Related security issues have to be analysed.
- Possibility for some applications/files to be restricted to one or some of the subscriptions, under user/SP control, with all applications that are shared, being done so in a secure manner.
- Inclusion of a payment method (electronic money and/or prepaid and/or subscription details)
- An interface allowing highly secure downloading and configuration of new functionality, new algorithms and new applications into the IC card as well as updating the existing applications, algorithms and data.
- Support for storing and possibly executing encryption related information, such as keys and algorithms.
- In multi application cards a functionality to prevent the unauthorised access and alteration of USIM specific information by other applications residing on the card.
- The ability to accept popular value-adding IC card applications, such as digital signature applications, EMV credit/debit card, electronic purses such as Mondex and Visacash, etc. Dynamic addition and deletion of these applications during the lifetime of the card is envisaged.
- Possibility for one UMTS SP to block multiple subscription on the card the SP has issued.

Shared applications could include databases (e.g. telephone books), service profiles (e.g. controlling divert information), users preferences (e.g. short dialling codes) and SP-specific parameters inside a USIM application (e.g. call barring tables).

6.3 Presence of an UMTS USIM

6.3.1 Using removable card for using UMTS services

The implications of the requirement that the UMTS IC card with a USIM must be physically present in the terminal at all times are:

1) It is of limited use to put applications other than the USIM on the UMTS IC card.

2) Multi-user terminals have to be multi-slot terminals, which limits personal mobility in UMTS.

3) Users have to carry multiple IC cards, which is not user friendly.

Therefore if the use of “swipe” cards could be facilitated in a secure manner it would benefit actors of the UMTS role model. The security concerns of the use of swipe cards in UMTS should be validated.

Examples of services that can be used without the permanent physical presence of the UMTS card in the terminal are:

- Services that are free of charge or are charged according to a flat rate.

- Services where the calling user does not require authentication of the intended recipient (which is a user option).

- The service concerns incoming communication for which the calling party has accepted all call charges. Therefore a prior registration is made for the service. To make the registration the IC card has to be present in the terminal.

6.3.2 Alternative payment methods

In current systems, the user identity and authentication functionality is the basis for charging. However, more choices for the user are already appearing, with many operators launching pre-paid and re-chargeable GSM-cards during this year. In the future, the acquisition and use of UMTS services should be as easy as possible. Alternative solutions should be available for paying for UMTS services and value-added services.

A large number of cards in your wallet is the reality today. Based on market demands smart card manufacturers are developing cards able to contain multiple applications on the single card. In future consumers, in conjunction with the card provider, will be able to construct a smart card which is able to hold a number of different applications to suit their individual requirements or lifestyle. These new applications may provide payment possibilities such as pre-paid, debit- or credit-card based applications. Smart card is ideal support for payment over the Internet, whether in cash or as credit. Smart card provides safe and movable place for the needed secret keys and allows only the right user to use it.

Pre-paid smart cards are probably the first phase in the development. Other possibilities will exist like electronic cheques or perhaps a straight access to bank. Mobile commerce is a fast evolving market and it is difficult to forecast future developments. The success of electronic and mobile commerce depends critically on user acceptance. It is not easy to change users’ habits, new payment methods must be easy to use.

6.3.3 Separation of USIM and the payment method

Another considered way of organising the UMTS security and service related information and the payment method in UMTS could be the usage of separate modules. UMTS specific security algorithms and information, i.e. the USIM application, could be contained by a security card (an IC Card, microchip or another security module), which would resolve the possible problems of authenticating the UMTS users and ciphering the user information using UMTS specific algorithms if required. The role of the separate security module depends of the final configuration. In case of an IC card acting as a security module, also authentication information (user specific) could be present, because of easy movability between different terminals. In case of a smaller HW based solution (silicon), which would be considered unremovable for daily purposes, only the ciphering functionality could be contained (system specific). At the same time the payment method required to access the UMTS services could be contained in another IC Card (Figure 1). Additionally following benefits have been identified:

- Given the anticipated use of UMTS for financial transactions it allows particular banks etc. to provide their own customised security on the removable IC card (including end-to-end security). This will normally be of higher assurance than GSM can currently provide. With the separate security module, there is no need for the financial institution to reveal the detail of their security algorithms to, for example ETSI or an equipment manufacturer. Instead they can provide a sub-system with a defined interface.

- It would help UMTS to provide some PMR-like services where user groups (e.g. law enforcement agencies) often require specific security provision (especially for encryption). This would be facilitated by permitting the insertion of the removable IC card. The EP-TETRA model may offer some useful insight into this functional separation.

- Possibility to have small terminals where the size is not restricted by the size of the IC card.

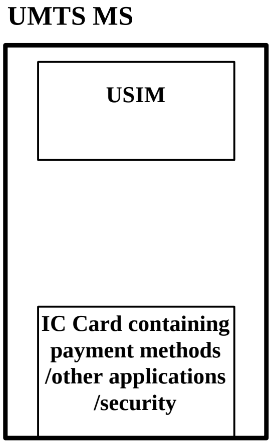

Figure 1: Separation of USIM and payment information

6.3.4 Separation of IC Card from the terminal equipment

In GSM terminology minimum configuration of a mobile station (MS) consists of a mobile equipment (ME) and a SIM card (Figure 2a). The introduction of mobiles with PCMCIA data functionality already makes this definition a little fuzzy (Figure 2b). In the context of UMTS, one could consider a possibility of UMTS terminals consisting of a laptop, radio PCMCIA card and a separate IC card reader (Figure 2c). The interface between the UMTS radio card and the IC card reader could be purely a software interface. This type of an MS configuration would raise following questions:

- Is this a valid configuration?

- Does the interface between UMTS radio card and a IC card reader have to be specified?

- Does the IC card have to be available for the whole time?

- Does the terminal know if the IC card has been removed from the reader?

- Would it be more viable in this configuration to use credit/debit/emoney card?

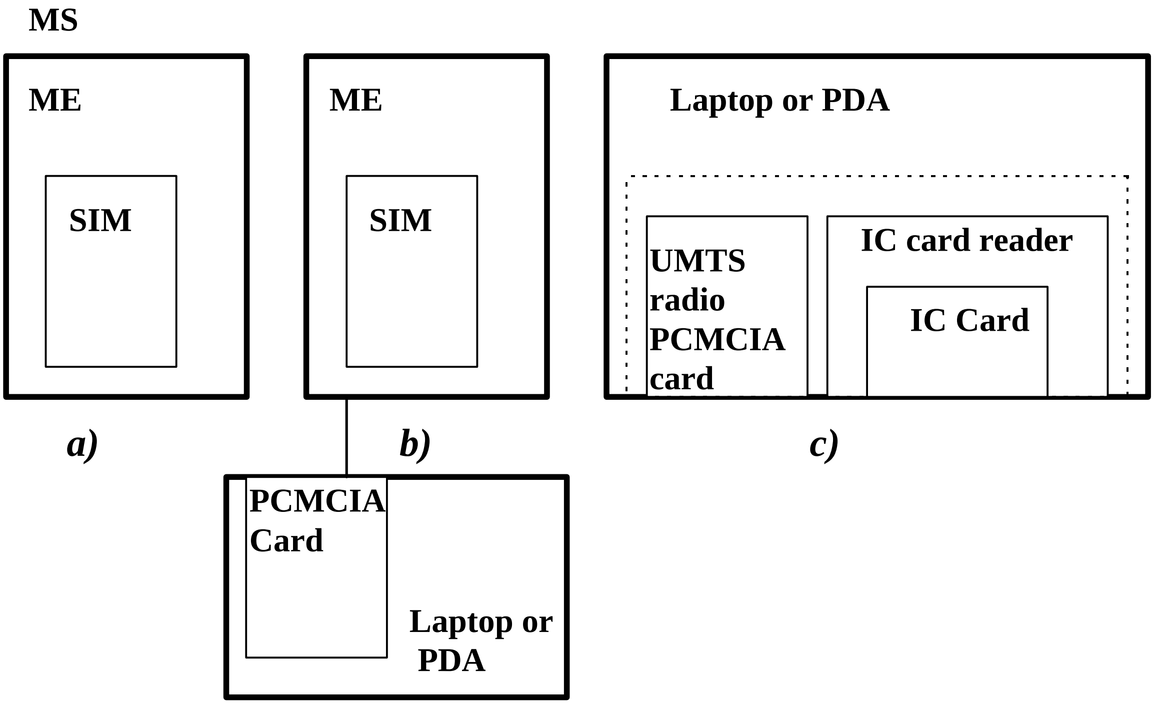

Figure 2: Examples of UMTS terminal configurations

6.4 Charging and accounting algorithms on the IC Card

For more information, please refer to ETSI UMTS 22.24.

7 Terminal Functionality

The UMTS standard does not restrict the functionality of the terminals in any way. The standard should allow terminal specific features and functions to exist. However, a minimum set of mandatory functions are required in order to ensure proper behaviour of the system.

7.1 Mandatory functions

The mandatory functionality of UMTS terminals is related mainly to the interaction between the terminal and the network. The following functions should be considered mandatory for all UMTS terminals:

- Terminal IC Card interface;
- SP and Network registration and deregistration;
- Location update;
- Originating or receiving a connection oriented or a connectionless service;
- An unalterable equipment identification;
- Basic identification of the terminal capabilities;
- Terminals capable for emergency calls should support emergency call without a USIM;
- Support for the execution of algorithms required for authentication and encryption;

7.2 Extra features

The Standard should support the following additional functionality for UMTS terminals:

- a mechanism to download service related information (parameters, scripts or even software), new protocols, other functions and even new APIs into the terminal;
- an API interface capability to allow information transfer through a well known interface;
- maintenance of the VHE using the same user interface and or another interface while roaming;
- optional insertion of several cards. An example scenario for this feature is a fax machine with a multiple IC card slots, where several users could insert their IC card and receive faxes.

7.3 External interfaces

Interfaces are needed for messages and information to be transferred between the terminal and an external device, e.g. a computer. Standardised interfaces and protocols shall be used as much as possible and UMTS specific enhancements will be specified for those. Additional physical specifications should not be specified by UMTS standards if possible.

External logical interfaces important for UMTS terminals can be, e.g. AT-command set, a SW API for PC environment.

7.4 Identification of Terminal capabilities

In the UMTS environment a large number of different terminal types are envisaged. All terminals will have to support mandatory functions identified for UMTS terminals (see subclause 7.1). One of the mandatory functions will be the identification of the terminal’s capabilities. Information provided in the identification of terminal capabilities should contain the used selections in the case where alternatives are available (e.g. which speech codecs are supported) as well as the optional functions and features important from the used service point of view (e.g. certain data compression algorithm supported). Early identification of terminal capabilities will save network resources, e.g. in the case of an intended call between two incompatible terminals.

As UMTS is intended to be a future proof system evolving in the future, all capabilities of the UMTS terminals cannot be identified and classified in the first phase of standardisation. Therefore, a basic classification of terminal capabilities is needed. UMTS terminals should identify their basic capabilities when attaching to the network. Further negotiation of enhanced capabilities and features will have to be carried out between the calling parties and applications.

Basic capabilities identified by the terminals could be e.g.:

- Supported speech codec: GSM, GSM EFR, AMR, proprietary, none, etc.
- Supported display type: character, graphic, none, etc.
- Radio capabilities: capable of listening in several network simultaneously, transmitting in several networks simultaneously, etc.

8 IC Card/Terminal Interfaces

8.1 The IC Card interface

An interface between the terminal and the IC Card should be standardised from the physical and functional point of view. The following characteristics are identified for the physical interface:

- Physical interface should be based on ISO - 7816 [2, 3, 4, 5]

- Future terminal and IC card technology development should be considered for efficient implementation. Such aspects as supply voltage levels (3V and less), interface bit rates, virtual-machine APIs and even contactless interfaces.

- The IC card physical interface should support high bit rate transmission in order to support efficiently the applications on the IC card.

The IC card physical interface should support invocation and data manipulation of USIM application and other IC card applications.

8.2 Internal Application Execution Interface

Execution of service provider specific services and applications will be supported by UMTS terminals. An API will be standardised for the purpose of hiding terminal specific implementation issues and support for the execution of downloadable services. In order to support execution of external applications, a script or a description language will have to be identified. UMTS specific script languages should be avoided to maintain compatibility and therefore similar developments from other environments such as computer and PDA environments should be closely investigated. A detailed study of the application execution environment requirements have been done [6]. Following list describes the major requirements to be supported by UMTS application execution environment:

- Application development independent of the terminal platform;

- Wide variety of application tailored for certain categories of terminals, e.g. low end and high end terminals;

- Support for sophisticated user interface and wide variety of MMI concepts;

- The means to support SP and VASP specific services;

- The means to download new services/functions into the terminal and upgrade existing services/functions;

8.3 Physical dimensions

One of the principles of UMTS is to provide personal and terminal mobility. Therefore, a user should be able to roam either with a terminal or an IC Card upon which resides a USIM. The IC Card should therefore have physical dimensions which facilitate portability. For example, the IC Card could have the physical dimensions of a credit card.

It should not be obligatory for a terminal to fully envelop an IC Card, it may be enough that the terminal simply covers that part of the card that contains the chip *(USIM?).*

It should be possible to have smaller IC cards that remain embedded in terminals.

In light of the above requirements, UMTS shall adopt both of the card formats currently used by GSM, i.e. the full-size ID1 format [EN 27810-1:1989], and the ID000 “plug-in” format [ENV 1375-1: 1994].

9 Testing and Type approval issues

Testing and type approval of the UMTS terminals should concentrate on the UMTS specific issues of the terminals, i.e. radio, protocols and UMTS specific functionality. Type approval should be included in to the standardisation process in a manner that does not cause extra delays to the introduction of terminals. Specific requirements for testing and type approvals will be defined later.

10 Conclusions

This ETSI report has presented concepts related to UMTS terminal and IC card usage. Based on the these concepts UMTS requirements for terminals and IC cards are also presented. Some of the concepts presented in this documents are not fully investigated and therefore more requirements might come up, after further evaluating those concepts that will be found useful by the SMG and evaluated by the SMG STCs. Also it has to be considered that in certain countries offering UMTS services, operators, regulators or legal authorities might restrict or recommend the usage of some of these concepts.

It is proposed that following UMTS IC card related standardisation activities will be carried out targeting to GSM/UMTS release 1999 (UMTS phase 1):

1) Mandatory functionality for the IC card containing a USIM application (see subclause 6.1).

2) Possibility to have also other applications on the IC card. Standardisation is needed to support the required functionality (see subclause 6.2 for relevant requirements).

3) Possibility to use alternative payment methods (see subclause 6.4.2).

4) Separation of USIM and the payment method (see subclause 6.3.3).

It is proposed that following UMTS terminal related standardisation activities will be carried out targeting to GSM/UMTS release 1999 (UMTS phase 1):

1) Mandatory functionality for the terminal (see subclause 7.1).

2) Mechanism to download service/function related information and SW (see subclause 7.2).

3) Application execution environment/interface (see subclause 8.2).

4) Mechanism to identify terminal capabilities related to services (see subclause 7.4).

It is proposed that following concepts will be part of UMTS phase 2 standardisation:

- Using removable card (e.g. swipe card) for using UMTS services (if security concerns can be resolved, see subclause 6.3.1).

- Multiple USIMs on single IC Card.

- Combination of concepts “Separation of USIM and the payment method (6.3.3)” and “Using removable card for

Separation of IC card reader from the terminal equipment (see subclause 6.3.4).

Annex A: Change history

Change history					
SMG No.	**TDoc. No.**	**CR. No.**	**Section affected**	**New version**	**Subject/Comments**
SMG#25				3.0.0	Approved at SMG#25 March 17-20, 1998
SMG#27	98-0581	A001	Sections 4, 6, 10	3.1.1	Security aspects relative to USIM & Payment methods.

History

Document history		
V3.0.0	February 1998	Unpublished
V3.1.1	November 1998	Unpublished
March 1999	V3.1.2	Version 3.1.2 Editorial format change for 3GPP