ETSI TR 131 900 V8.0.0 (2009-03)

Technical Report

Universal Mobile Telecommunications System (UMTS);
LTE;
SIM/USIM internal and external interworking aspects
(3GPP TR 31.900 version 8.0.0 Release 8)

Reference

RTR/TSGC-0631900v800

Keywords

LTE, UMTS

ETSI

650 Route des Lucioles
F-06921 Sophia Antipolis Cedex - FRANCE

Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Siret N° 348 623 562 00017 - NAF 742 C
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° 7803/88

Important notice

Individual copies of the present document can be downloaded from:
http://www.etsi.org

The present document may be made available in more than one electronic version or in print. In any case of existing or perceived difference in contents between such versions, the reference version is the Portable Document Format (PDF). In case of dispute, the reference shall be the printing on ETSI printers of the PDF version kept on a specific network drive within ETSI Secretariat.

Users of the present document should be aware that the document may be subject to revision or change of status. Information on the current status of this and other ETSI documents is available at
http://portal.etsi.org/tb/status/status.asp

If you find errors in the present document, please send your comment to one of the following services:
http://portal.etsi.org/chaircor/ETSI_support.asp

Copyright Notification

No part may be reproduced except as authorized by written permission.
The copyright and the foregoing restriction extend to reproduction in all media.

© European Telecommunications Standards Institute 2009.
All rights reserved.

DECTTM, **PLUGTESTS**TM, **UMTS**TM, **TIPHON**TM, the TIPHON logo and the ETSI logo are Trade Marks of ETSI registered for the benefit of its Members.
3GPPTM is a Trade Mark of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners.
LTE™ is a Trade Mark of ETSI currently being registered
for the benefit of its Members and of the 3GPP Organizational Partners.
GSM® and the GSM logo are Trade Marks registered and owned by the GSM Association.

Intellectual Property Rights

IPRs essential or potentially essential to the present document may have been declared to ETSI. The information pertaining to these essential IPRs, if any, is publicly available for **ETSI members and non-members**, and can be found in ETSI SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available from the ETSI Secretariat. Latest updates are available on the ETSI Web server (http://webapp.etsi.org/IPR/home.asp).

Pursuant to the ETSI IPR Policy, no investigation, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in ETSI SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

Foreword

This Technical Report (TR) has been produced by ETSI 3rd Generation Partnership Project (3GPP).

The present document may refer to technical specifications or reports using their 3GPP identities, UMTS identities or GSM identities. These should be interpreted as being references to the corresponding ETSI deliverables.

The cross reference between GSM, UMTS, 3GPP and ETSI identities can be found under http://webapp.etsi.org/key/queryform.asp.

Contents

Intellectual Property Rights 2
Foreword 2
Foreword 5
Introduction 5
1 Scope 6
2 References 6
3 Abbreviations 7
4 Primary clarifications and definitions 7
4.1 2G and 3G 7
4.2 SIM, USIM and UICC 8
4.3 Types of ME 8
4.4 Types of VLR/SGSN and HLR/AuC 8
4.5 Security related terms 9
5 Interworking between the ME and the ICC 9
5.1 3G ME and UICC 10
5.2 2G ME and UICC 11
5.2.1 2G ME of Rel-4 (or earlier) without USIM support 11
5.2.2 2G ME of R99 or Rel-4 with USIM support or of Rel-5 11
5.3 3G ME and SIM 11
5.3.1 3G ME of R99 or Rel-4 11
5.3.2 3G ME of Rel-5 11
5.4 2G ME and SIM 12
5.4.1 2G ME of Rel-4 (or earlier) 12
5.4.2 2G ME of Rel-5 12
6 Authentication and key agreement in mixed networks 12
6.1 With 3G ME and UICC 12
6.2 With 2G ME and UICC 15
6.2.1 2G ME of Rel-4 (or earlier) without USIM support 15
6.2.2 2G ME of R99 or Rel-4 with USIM support or of Rel-5 17
6.3 With 3G ME and SIM 19
6.3.1 3G ME of R99 or Rel-4 19
6.3.2 3G ME of Rel-5 21
6.4 With 2G ME and SIM 21
6.4.1 2G ME of Rel-4 (or earlier) 21
6.4.2 2G ME of Rel-5 22
7 Interworking between a SIM application and a USIM application on a UICC 23
7.1 IMSI, secret key and authentication algorithm 23
7.2 File mapping 24
7.3 Access conditions 24
7.4 Secret codes 24
7.5 Activation of 2G and 3G operation modes 25
7.6 Selection of cyclic files 26
7.7 Enabling/disabling procedures for dialling numbers 26
8 Interworking between USIM applications on a UICC 27
9 SIM and UICC Interworking on the Card/Terminal Interface 27
Annex A: Interworking table 29
Annex B: Features for security interworking 33

B.1 Conversion functions....33
B.2 3G algorithm execution modes....33

Annex C: SIM/USIM file mapping table....35

Annex D: CHV mapping....37
D.1 In a single-verification capable UICC....38
D.2 In a multi-verification capable UICC (static mapping)....38
D.3 In a multi-verification capable UICC (dynamic mapping)....38

Annex E: Change history....40

History....41

Foreword

This Technical Report has been produced by the 3rd Generation Partnership Project (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 the present document, 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: or greater 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 document.

Introduction

This document describes the different cases of interaction between an Identity Module (GSM-SIM or a 3G-UICC) and a GSM or 3G mobile equipment with a special focus on the diverse situations that can apply in a mixed 2G/3G network environment.

Depending on the technical properties of other involved network elements, particularly during authentication and key agreement, the ICC and the ME may or must support some specific features to allow for compatibility. This is a complex matter and has generated some amount of confusion as the basic conditions implied by the 3G UICC are not always as clearly understood as they should be. The present document gives guidance by summarising the important details and applying them to the (theoretically) possible cases of security interworking along the transmission chain.

The document further tries to explain the options of interworking that exist internally when a SIM and one or more USIM(s) are implemented together on a single UICC.

As this document is a technical report and not a technical specification, none of its contents have the character of a requirement. Merely they should be seen as a clarifying summary and straightforward interpretation of the underlying core specifications.

1 Scope

The present document describes

- the different cases of interworking between a 2G or 3G ICC and a 2G or 3G ME.
- the different cases of interworking between any given ME/ICC combination and the rest of the network
- the possibilities of interworking between a SIM and a USIM together on a single UICC
- the possibilities of interworking between several USIMs on a single UICC

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 TS 31.101: "UICC-Terminal Interface; Physical and Logical Characteristics".

[2] 3GPP TS 31.102: "Characteristics of the USIM Application".

[3] 3GPP TS 21.111: "USIM and IC Card Requirements".

[4] 3GPP TS 22.100: "UMTS Phase 1".

[5] 3GPP TS 22.101: "Service Aspects; Service Principles".

[6] 3GPP TS 33.102: "3G Security; Security Architecture".

[7] 3GPP TS 11.11: "Specification of the Subscriber Identity Module - Mobile Equipment Interface".

[8] 3GPP TS 51.011: "Specification of the Subscriber Identity Module - Mobile Equipment Interface".

3 Abbreviations

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

2G	2nd Generation
3G	3rd Generation
AKA	Authentication and Key Agreement
AuC	Authentication Centre
AUTN	Authentication Token
BSS	Base Station Subsystem
CHV	Card Holder Verification
CK	Ciphering Key in 3G
DF	Dedicated File
EF	Elementary File
GERAN	GSM/EDGE Radio Access Network
GSM	Global System for Mobile Communication
HLR	Home Location Register
ICC	Integrated Circuit Card
IK	Integrity Key
IMSI	International Mobile Subscriber Identity
K	Secret Key in 3G
Kc	Ciphering Key in 2G
Ki	Secret Key in 2G
MAC	Message Authentication Code
ME	Mobile Equipment
PIN	Personal Identification Number
RAND	Random Challenge
RES	Authentication value returned by the USIM in 3G AKA or delivered by the 2G HLR/AuC
SGSN	Serving GPRS Support Node
SIM	Subscriber Identity Module
SRES	Authentication value returned by the SIM or by the USIM in 2G AKA
SQN	Sequence Number
TS	Technical Specification
TR	Technical Report
UICC	Universal Integrated Circuit Card
UMTS	Universal Mobile Telecommunication System
USIM	Universal Subscriber Identity Module
VLR	Visitor Location Register
XMAC	Expected Message Authentication Code calculated in the USIM in 3G AKA
XRES	Expected Authentication value delivered by the 3G HLR/AuC

4 Primary clarifications and definitions

For the purpose of this report, the following clauses clarify the meaning of some important terms.

4.1 2G and 3G

The abbreviation 2G stands for 2nd generation technology and characterises elements of a mobile communication system which are based on the GSM standard, i.e. 2G technical specifications or their equivalent successors under the 3GPP administration. A 2G entity only comprises the mandatory and optional functionality specified in GSM and does not ensure any forward compatibility with 3G, with a particular exception: 2G terminals of R99 and Rel-4 may and from Rel-5 onwards have to support the 3G USIM.

The abbreviation 3G stands for 3rd generation technology and characterises elements of a mobile communication system which are based on 3GPP technical specifications. A 3G entity only comprises the mandatory and optional functionality specified in 3G, features for 2G backward compatibility are only included if explicitly required by the relevant 3G specifications.

Some 3G specifications differentiate the functional extent of a mobile network entity between releases 98 and earlier (R98-) and releases 99 and later (R99+). As for example a GSM ME exists in both release categories while a 3G ME is only defined from release 99 onwards, this split does not make sense without mentioning the respective technology. For the purpose of this document it therefore appears more appropriate to differentiate between 2G and 3G only, with the relationship given by

2G = GSM = GSM R98- or GSM R99+

3G = 3G R99+

4.2 SIM, USIM and UICC

The most general term for a smart card, i.e. a micro-controller based access module, not only for mobile communication purposes, is "ICC". It is always a physical and logical entity and, in the context of this document, either a SIM or a UICC.

The SIM is the ICC defined for 2G. It has originally been specified as one physical and logical entity, not distinguishing platform and application. In 3G, the SIM may also be an application on the 3G UICC, then of course only represented by its logical characteristics. If the SIM application is active, the UICC is functionally identical to a 2G SIM. The SIM (or SIM application on a UICC) does only accept 2G commands. It is specified in GSM TS 11.11 [7] / TS 51.011 [8].

Unlike the SIM, the USIM is not a physical entity, but a purely logical application that resides on a UICC. It does only accept 3G commands and is therefore not compatible with a 2G ME. The USIM may provide mechanisms to support 2G authentication and key agreement to allow a 3G ME to access a 2G network. It is specified in 3G TS 31.102 [2].

The UICC is the physical and logical platform for the USIM. It does at least contain one USIM application and may additionally contain a SIM application. Further to that, the UICC may contain additional USIMs and other applications, e.g. for mobile banking or mobile commerce purposes, if these fit with the basic physical and logical characteristics of the UICC. It is specified in 3G TS 31.101 [1].

4.3 Types of ME

For the purpose of this document, the following definitions apply for the ME:

- A 3G ME is either a 3G single mode ME that only supports a 3G radio access network or a 2G/3G dual mode ME that supports both, a 2G radio access network (GSM) and a 3G radio access network, which ever is present. In either case it can handle 3G AKA and 2G AKA and is able to interwork with either a USIM application on a UICC or a SIM. For better understanding, explicit usage of the term "2G/3G dual mode ME" points out particular requirements.
- A 2G ME does only support a 2G radio access network (GSM).
    - If it is of R98 or earlier, it can only handle 2G AKA and is only able to interwork with either a SIM application on a UICC or a SIM. Then the card interface complies to GSM TS 11.11 [7].
    - If it is of R99 or Rel-4, it can handle 2G AKA and is able to interwork with either a SIM application on a UICC or a SIM. Then the card interface complies to GSM TS 11.11 [7] / TS 51.011 [8]. Additionally, it may support 3G AKA and be capable to interwork with a USIM application on a UICC. In this optional mode, the card interface complies to 3G TS 31.101 [1] and 3G TS 31.102 [2].
    - If it is of Rel-5 or later, it can handle 2G AKA and 3G AKA (depending on the current network situation) and is capable to work with a USIM application on a UICC. On the card interface, it behaves just like a 3G ME, i.e. it complies to 3G TS 31.101 [1] and 3G TS 31.102 [2]. As a recommended option, the 2G ME of Rel-5 and onwards may additionally support a 2G SIM.

4.4 Types of VLR/SGSN and HLR/AuC

For the purpose of this document, the following definitions apply for the VLR/SGSN and HLR/AuC:

- A 2G HLR/AuC supports triplet generation for 2G subscriptions, but does not support quintet generation. Only 2G AKA can be performed. A triplet consists of RAND, RES and Kc, while a quintet comprises RAND, XRES, CK, IK and AUTN. A 2G HLR/AuC does not support any conversion functions.

- A 3G HLR/AuC supports quintet generation for 3G subscriptions. To support 2G AKA, i.e. to convert quintets into triplets, it shall support conversion functions c2 and c3 as defined in 3G TS 33.102 [6]. It may additionally support pure triplet generation for 2G subscriptions.

- A 2G VLR/SGSN only supports 2G AKA and can only be attached to a 2G BSS. It does not support any conversion functions.

- A 3G VLR/SGSN supports 3G AKA and 2G AKA. It can be attached to a 3G BSS and/or a 2G BSS. To convert quintets from a 3G HLR/AuC into triplets necessary for 2G AKA, it shall support conversion functions c2 and c3 as defined in 3G TS 33.102 [6].

4.5 Security related terms

2G AKA is the procedure to provide authentication of an ICC to a serving network domain and to generate the key Kc in accordance to the mechanisms specified in TS 03.20. In a mixed 2G/3G network environment 2G AKA is performed when - except for the BSS - at least one other element is 2G.

3G AKA is the procedure to provide mutual authentication between an ICC and a serving network domain and to generate the keys CK and IK in accordance to the mechanisms specified in 3G TS 33.102 [6]. For 3G AKA all involved elements - except for the BSS - have to be 3G.

2G Security Context is a state that is established between a user and a serving network domain (i.e. between the ICC and the VLR/SGSN) after the execution of 2G AKA, with ciphering Kc available at either side.

3G Security Context is a state that is established between a user and a serving network domain (i.e. between the ICC and the VLR/SGSN) after the execution of 3G AKA, with ciphering and integrity protection keys CK and IK available at either side. 3G Security Context is still given, if these keys are converted into Kc to work with a 2G BSS.

5 Interworking between the ME and the ICC

The 3G system is designed to be compatible with GSM and several interworking requirements apply. Regarding the ICC/ME interface, some basic requirements can be identified in the 3G standards. They are differing between the subsequent releases:

For R99, the following applies:

- In 3G TS 22.100 [4]: "The UMTS mobile terminal shall support phase 2 and phase 2+ GSM SIMs as access modules to UMTS networks." In other words: A R99 3G ME shall support a 2G ICC.

- In 3G TS 22.101 [5]: "It shall be possible to use the UICC in 2G terminals to provide access to GSM networks. In order to achieve that option, it shall be possible to store a module containing 2G access functionalities on the UICC which shall be accessed via the standard GSM SIM-terminal interface. " In other words: The R99 UICC may contain a SIM application.

- Additionally, a 2G terminal of R99 may provide a USIM interface. For Rel-4, 3G TS 22.100 [4] does not exist. There are however similar statements in 3G TS 22.101 [5]:

    - "The basic mandatory UE requirements are: Support for GSM phase 2 and 2+ SIM cards […]", meaning that also a Rel-4 ME does work with a 2G ICC.

    - "It shall be possible to use the UICC in 2G terminals to provide access to networks supporting GERAN (including networks based on earlier GSM specifications). In order to achieve that option, it shall be possible to store a module containing 2G access functionalities on the UICC, which shall be accessed via the standard SIM-terminal interface." In other words: The Rel-4 UICC may contain a SIM application.

    - Additionally, a 2G terminal of Rel-4 may provide a USIM interface.

Therefore, in R99 and Rel-4 we have the same situation. Note that it is not a mandatory requirement in R99 and Rel-4 that a USIM has to be supported by a 2G ME. However, it is optional and in addition to the 2G SIM interface. In order to allow a 3G UICC to work in a 2G ME where the USIM is not supported, it is feasible to put a SIM application (according to TS 11.11 [7] / TS 51.011 [8]) onto the UICC in addition to the USIM.

For Rel-5, the requirement for 2G MEs to support 2G ICCs was deleted from 3G TS 22.101[5], instead the following statements were inserted:

- "In Release 5 and later, terminals supporting only GERAN shall support USIM." with a note "It is strongly recommended that manufacturers implement SIM support on GERAN only terminals until the population of SIMs in the market is reduced to a low level."
- "The basic mandatory UE requirements are: Support for USIM. Optional support of GSM phase 2, 2+, 3GPP Release 99 and Release 4 SIM cards. […] Support for the SIM is optional for the UE, however, if it is supported, all the mandatory requirements for SIM shall be supported in the UE […]."

This means basically that for 2G and 3G MEs of Rel-5 the support of 2G SIMs is now optional and it is mandatory (in particular for the 2G ME) to support the USIM. Note that although a SIM application on the UICC is no longer mentioned, it is still essential (and certainly allowed) to support Rel-4 and earlier terminals that do not optionally accept a USIM with a SIM application on Rel-5 UICCs. In this case, the Rel-4 SIM specifications apply.

For the ICC/ME interface, with two main types of ME (3G and 2G) and two main types of ICC (UICC and SIM), four different scenarios can be identified. They are described in the following sections with appropriate splits into sub-sections if release specific differences have to be taken into account.

5.1 3G ME and UICC

Any 3G ME, independent of the release, has to support the UICC. 3G TS 31.101 [1] and 3G TS 31.102 [2] apply.

According to 3G TS 21.111 [3] a 3G ME does not support a 5V ME/UICC interface. As laid out in the same specification, a UICC does always support at least two voltage classes, i.e. a 5V only UICC cannot exist.

In case of a UICC inserted in a 3G ME, nothing but the 3G command set (as defined in 3G TS 31.101 [1] and 3G TS 31.102 [2]) can be used by the ME. In particular, the 2G command RUN GSM ALGORITHM is not available.

To support a 2G/3G dual mode ME in a 2G radio access network, the USIM may provide functions for 2G backward compatibility. Two particular USIM services are defined for such purposes:

1. **Service n° 27:** "GSM Access". This service is essential when a 2G BSS is involved and ciphering is active in the BSS. The USIM additionally generates the 2G ciphering key Kc required by the 2G air interface. From the security point of view, this behaviour can be characterised as "**3G + Kc mode**" (see below). Further, the USIM supports some additional 2G data storage elements that are necessary for 2G radio access. If service n° 27 is not available in the USIM, the lack of Kc prevents operation with a 2G BSS when ciphering is active. No ciphering key derivation is done by the ME.
2. **Service n° 38:** "GSM Security Context". This service is required when a 2G VLR/SGSN and/or a 2G HLR/AuC is involved. The USIM performs 2G AKA, i.e. it accepts 2G input data and generates 2G output data. From the security point of view, this behaviour can be characterised as "**virtual 2G mode**" (see below). If service n° 38 is not available in the USIM, 2G AKA is not supported and network access is impossible with a 2G VLR/SGSN and/or a 2G HLR/AuC.

   A 2G VLR/SGSN never goes with a 3G BSS. Hence when a 2G VLR/SGSN is involved, then a 2G BSS is always part of the transmission chain and service n° 27 is additionally required, i.e. services n° 27 and n° 38 have to be available at the same time.

If services n° 27 and n° 38 are not supported by the USIM (which the ME can detect from the USIM Service Table during the USIM activation procedure) network access is impossible in a mixed 2G/3G environment, even if a SIM application is available on the UICC. A 3G ME only accesses the USIM application on the UICC.

From the security point of view, the compatibility services are connected to up to three different operation modes (see also Annex B):

- **Normal 3G mode:** The results of the 3G algorithm are sent to the ME without any change. The USIM receives RAND and AUTN and responds with RES, CK and IK. This mode applies if service n° 27 is not available.

- **3G + Kc mode:** The 2G ciphering key Kc (derived from CK, IK) is additionally included in the response. The USIM receives RAND and AUTN and responds with RES, CK, IK and Kc. This requires conversion function c3 to be supported by the USIM. If service n° 27 is available in the USIM, this mode is always active and the ME picks the relevant values from the USIM response according to the present network situation.
- **Virtual 2G mode:** The USIM receives a 2G authentication request with RAND and returns a 2G authentication response with SRES (derived from RES) and ciphering key Kc (derived from CK, IK). This requires a particular algorithm execution mode plus conversion functions c2 and c3 to be supported by the USIM. If service n° 38 is available in the USIM, this mode is not always active. The ME may switch the USIM from normal 3G mode or 3G + Kc mode to virtual 2G mode by sending a particular command parameter according to the present network situation.

The services n° 27 and n° 38 are both optional. Network operators can decide whether to include them into their USIMs and hence to allow network access with lower security level. It should be noted that this access limitation also affects emergency call set-up and handover.

5.2 2G ME and UICC

As explained in the beginning of paragraph 5, the interworking of this combination is dependent on the actual specification release, the terminal complies to.

5.2.1 2G ME of Rel-4 (or earlier) without USIM support

A 2G ME of Rel-4 (or earlier) is not required to support a USIM, however in R99 and Rel-4 this is allowed as an option. If it does not support a USIM, this combination will only work if a SIM application is provided by the UICC. TS 11.11 [7] / TS 51.011 [8] applies.

5.2.2 2G ME of R99 or Rel-4 with USIM support or of Rel-5

A 2G ME of R99 or Rel-4 can and a 2G ME of Rel-5 must support the UICC and interwork with a USIM application on it. In this case, the mechanisms described in section 5.1 above apply with the following additional remark:

The USIM services n° 27 and n° 38 are still optional for the USIM. However, as a 2G ME can only access a 2G BSS, a 2G ciphering key Kc is always required and thus service n° 27 becomes mandatory. If further a 2G VLR/SGSN and/or a 2G HLR/AuC is involved (a common situation in 2G networks), service n° 38 is also necessary. It is therefore recommended to the card issuer who wants to support this ME/ICC combination to have both services activated in the USIMs.

5.3 3G ME and SIM

This combination is depending on the actual 3GPP release the terminal is compliant to.

5.3.1 3G ME of R99 or Rel-4

A 3G ME of R99 or Rel-4 supports a 2G SIM. For this purpose it has to provide 2G SIM interface in addition to the 3G UICC interface. Access is possible to both 3G and 2G networks. The services that can be provided in this case may be limited to GSM like services. It is up to the 3G network operator to accept or reject the use of GSM SIMs as access modules to his network. TS 11.11 [7] / TS 51.011 [8] applies.

According to 3G TS 21.111 [3] and TS 22.100 [4] a 3G ME does not support a 5V ME/UICC or a 5V ME/SIM interface. This means that a 3G ME is not compatible with 5V only SIMs.

5.3.2 3G ME of Rel-5

For a 3G ME of Rel-5 support of the 2G SIM is only optional. If this option is taken (strongly recommended as there are huge quantities of legacy 2G SIMs in almost all major markets), there is no difference to section 5.3.1. Otherwise this combination does not work.

5.4 2G ME and SIM

This combination is depending on the actual 3GPP release the terminal is compliant to.

5.4.1 2G ME of Rel-4 (or earlier)

This is the well-known 2G case. TS 11.11 [7] / TS 51.011 [8] applies. Access to 3G networks is not possible with this combination.

5.4.2 2G ME of Rel-5

For a 2G ME of Rel-5 support of the 2G SIM is only optional. If this option is taken (strongly recommended as there are huge quantities of legacy 2G SIMs in almost all major markets), there is no difference to section 5.4.1. Otherwise this combination does not work.

6 Authentication and key agreement in mixed networks

The authentication and key agreement procedure basically involves five network components (ICC, ME, BSS, VLR/SGSN and HLR), each of which can be either 2G or 3G. Not all combinations work due to missing compatibility, and some require specific support by the ICC. The following sections give an overview on the theoretically possible combinations when a given ICC/ME pair is used. Again, release-dependent differences on the ME side have to be taken into account. A summary list is included in Annex A.

6.1 With 3G ME and UICC

When both ICC and ME are 3G (i.e. the ICC is a UICC), eight different combinations (security scenarios) of the other three network components remain. They are given in the following table:

Case	ICC	ME	BSS	VLR/SGSN	HLR/AuC	Service	Figure 1
1	3G	3G (any release)	3G	3G	3G	yes	A
2			2G	3G	3G	yes 1) 3)	B
3			3G	2G	3G	no	
4			2G	2G	3G	yes 2) 3)	C
5			3G	3G	2G	no	F
6			2G	3G	2G	yes 2) 3)	E
7			3G	2G	2G	no	
8			2G	2G	2G	yes 2) 3)	D

Note: 1) requires service n° 27 supported by the USIM
2) requires services n° 27 and n° 38 supported by the USIM
3) only with 2G/3G dual mode ME

Case 1: All system elements are 3G and thus capable of handling the related security mechanisms. 3G AKA is executed and 3G security context established. The USIM receives parameters RAND and AUTN and responds with RES, CK and IK.

NOTE: If service n° 27 is active in the USIM (to support mixed 2G/3G scenarios), Kc is generated by conversion function c3 and additionally included in the response. However, Kc is not needed in this security scenario and can be discarded by the ME.

This scenario is marked with A in figure 1.

Case 2: All system elements are 3G, except for the radio interface, which is 2G. This applies when a 3G subscriber roams into a 2G radio access network, which is connected to a 3G VLR/SGSN (e.g. when in the start phase of a 3G network not yet all existing 2G BSS are replaced by 3G technology, while the VLR/SGSN is already 3G).

3G AKA is executed. The 2G BSS is transparent for 3G authentication parameters but not capable of handling ciphering and integrity protection keys CK and IK. Therefore the 3G VLR/SGSN and the 3G ICC have to compute Kc from CK, IK with conversion function c3 and send it to the BSS and to the ME. Despite a 2G radio access network is involved, 3G security context is established. No service with a 3G single mode ME.

The USIM receives parameters RAND and AUTN and calculates RES, CK and IK. If service n° 27 is available, Kc is generated by conversion function c3 and additionally included in the response. The keys CK and IK are not needed in this security scenario and can be discarded by the ME. If the USIM does not support service n° 27, network access is not possible.

This scenario is marked with B in figure 1.

Case 3: All system elements are 3G, except for the VLR/SGSN which is 2G. As a 2G VLR/SGSN and a 3G BSS are not compatible, this theoretical combination cannot exist. No service in this case.

Case 4: ME, ICC and HLR/AuC are 3G, BSS and VLR/SGSN are 2G. This applies when a 3G subscriber roams into a 2G network - a very common case as networks will introduce 3G technology at different times or not at all.

Upon request by a 2G VLR/SGSN the 3G HLR/AuC produces 2G triplets RAND, RES, Kc out of 3G quintets RAND, XRES, CK, IK, AUTN. It therefore applies conversion function c2 to generate RES from XRES and conversion function c3 to generate Kc from CK and IK. RAND is left unchanged and AUTN is discarded. The 2G triplet is then sent to the VLR/SGSN. Between the VLR/SGSN and the USIM 2G AKA is executed, i.e. using RAND in the request and SRES in the response. No service with a 3G single mode ME.

To handle 2G AKA, the USIM must be capable to accept a request with RAND and return a response with SRES and Kc. The support of the virtual 2G mode is indicated by service n° 38 in the USIM Service Table. Since a 2G BSS is involved, service n° 27 is also necessary. In case the USIM does not support services n° 27 and n° 38, network access is not possible.

This scenario is marked with C in figure 1.

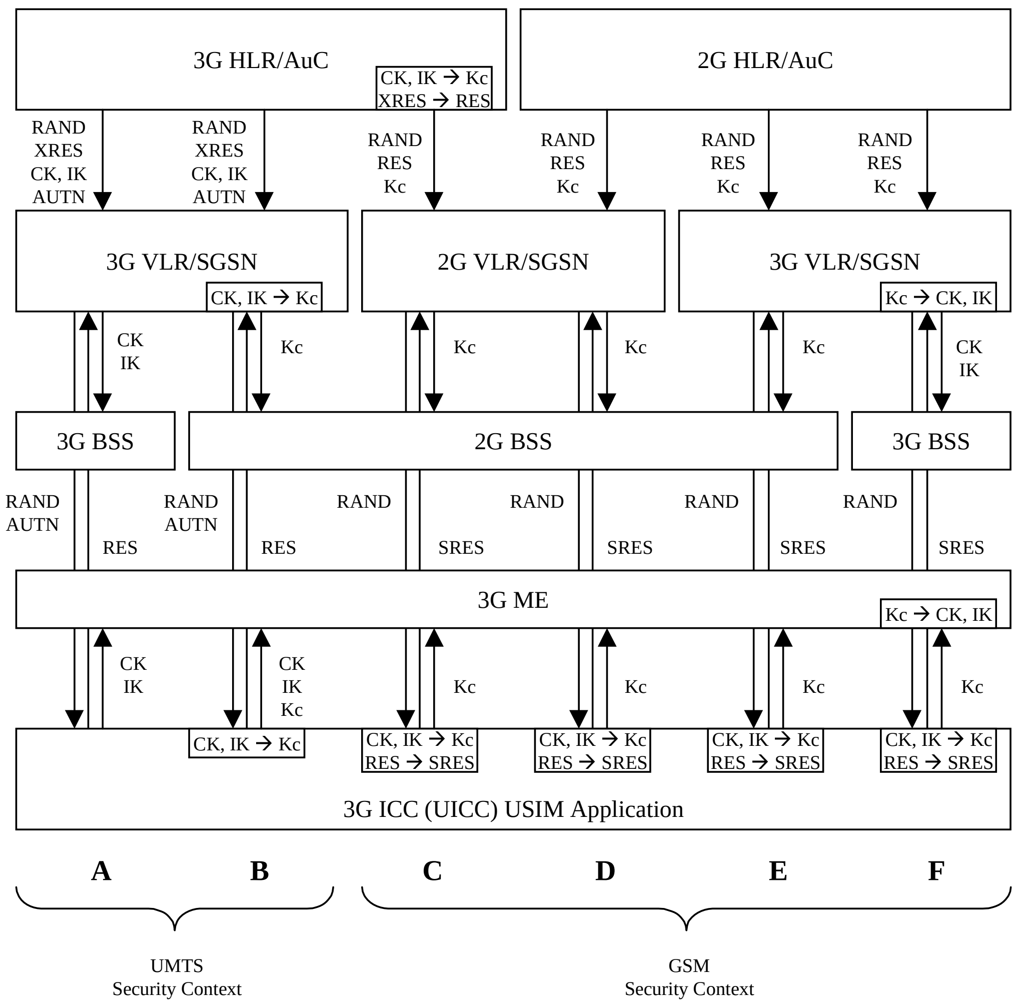

3G HLR/AuC
CK, IK → Kc
XRES → RES
2G HLR/AuC
RAND XRES CK, IK AUTN
RAND XRES CK, IK AUTN
RAND RES Kc
RAND RES Kc
RAND RES Kc
RAND RES Kc
3G VLR/SGSN
CK, IK → Kc
2G VLR/SGSN
3G VLR/SGSN
Kc → CK, IK
CK IK
Kc
Kc
Kc
Kc
CK IK
3G BSS
2G BSS
3G BSS
RAND AUTN
RES
RAND AUTN
RES
RAND
SRES
RAND
SRES
RAND
SRES
RAND
SRES
3G ME
Kc → CK, IK
CK IK
CK IK Kc
Kc
Kc
Kc
Kc
CK, IK → Kc
CK, IK → Kc
RES → SRES
CK, IK → Kc
RES → SRES
CK, IK → Kc
RES → SRES
CK, IK → Kc
RES → SRES
3G ICC (UICC) USIM Application
A
B
C
D
E
F
UMTS Security Context
GSM Security Context

Figure 1: Possible interworking scenarios of a 3G ME and UICC with different network environments

Case 5: All system elements are 3G, except for the HLR/AuC, which is 2G. This scenario would result into 2G AKA, but although the necessary conversions would be technically feasible, this combination is not a valid option as it would violate a basic security requirement in 3G TS 33.102 [6]: A 3G ME with a UICC inserted with a USIM activated and attached to a 3G BSS shall only participate in 3G AKA and shall not participate in 2G AKA. Accordingly the ME shall deny service in this case.

This scenario is marked with F in figure 1.

NOTE: There is one main consequence from this scenario: If a network operator issues UICCs in order to enable his customers to use a 3G access network (at home or while roaming), the related subscriptions should be installed in a 3G HLR/AuC. Otherwise authentication will fail as a 3G ME should not participate in 2G AKA.

Case 6: All system elements are 3G, except for the BSS and the HLR/AuC, which are 2G. It is possible to keep a 3G subscription in a 2G HLR/AuC, however on request by a 3G VLR/SGSN this can only deliver 2G triplets RAND, RES and Kc. The 3G VLR/SGSN is backward compatible and behaves like a 2G VLR/SGSN: Between the VLR/SGSN and the USIM 2G AKA is executed, i.e. using RAND in the request and SRES in the response. No service with a 3G single mode ME.

To handle 2G AKA, the USIM must be capable to accept a request with RAND and return a response with SRES and Kc. The support of the virtual 2G mode is indicated by service n° 38 in the USIM Service Table. Since a 2G BSS is involved, service n° 27 is also necessary. In case the USIM does not support services n° 27 and n° 38, network access is not possible.

This scenario is marked with E in figure 1.

Case 7: All involved system elements are 3G, except for the VLR/SGSN and the HLR/AuC, which are 2G. The situation is the same as in case 3 above: As a 2G VLR/SGSN a 3G BSS are not compatible, this theoretical combination cannot exist. No service in this case.

Case 8: ICC and ME are 3G and BSS, VLR/SGSN and HLR/AuC are 2G. The situation is actually very similar to case 4, but here the 2G HLR/AuC is delivering the necessary 2G triplets directly. No service with a 3G single mode ME.

Again this mixed network environment requires the virtual 2G mode in the USIM, indicated by service n° 38. As a 2G BSS is involved, service n° 27 is also necessary. If the USIM does not support services n° 27 and n° 38, network access is not possible.

This scenario is marked with D in figure 1.

6.2 With 2G ME and UICC

6.2.1 2G ME of Rel-4 (or earlier) without USIM support

When the ME is 2G and of Rel-4 (or earlier) and does not support a USIM while the ICC is 3G (i.e. it is a UICC), this pair will only interoperate if a SIM application is provided by the UICC. The USIM application is not relevant in this case. Again eight different combinations of the remaining three network components are existing. They are given in the following table:

Case	ICC	ME	BSS	VLR/SGSN	HLR/AuC	Service	Figure 2
1	3G with SIM Appl.	2G (without USIM support)	3G	3G	3G	no	
2			2G	3G	3G	yes 1)	G
3			3G	2G	3G	no	
4			2G	2G	3G	yes 1)	H
5			3G	3G	2G	no	
6			2G	3G	2G	yes 1)	J
7			3G	2G	2G	no	
8			2G	2G	2G	yes 1)	I
Note: 1) No service if UICC does not contain a SIM application							

Cases 1, 3, 5, 7: A 2G ME cannot interwork with a 3G BSS. Further, in cases 3 and 7, a 3G BSS does not work in combination with a 2G VLR/SGSN. No service in these cases.

Case 2: ME and BSS are 2G, the rest is 3G. This applies when a 3G subscriber with a 2G ME roams into a 2G radio access network, which is connected to a 3G VLR/SGSN (e.g. when in the start phase of a 3G network not yet all of the existing 2G BSS is replaced by 3G technology, while the VLR/SGSN is already 3G).

Upon request from a 3G VLR/SGSN, the 3G HLR/AuC delivers quintets. The VLR/SGSN, as it does not know what type of ME it is communicating with, forwards RAND and AUTN. The 2G ME simply ignores AUTN, therefore the UICC only receives RAND and responds with SRES for 2G AKA. After determination that 2G AKA is to be executed, the 3G VLR/SGSN generates Kc from CK/IK (conversion function c3) and RES from XRES (conversion function c2). It then also performs 2G AKA. In the UICC only the SIM application is active.

This scenario is marked with G in figure 2.

Case 4: ME, BSS and VLR/SGSN are 2G, ICC and HLR/AuC are 3G. This applies when a 3G subscriber with a 2G ME roams into a 2G network.

Upon request from a 2G VLR/SGSN, the 3G HLR/AuC must produce 2G triplets out of 3G quintets. It therefore applies conversion function c2 to generate RES from XRES and conversion function c3 to generate Kc from CK, IK. RAND is left unchanged and AUTN is discarded. The 2G triplet is sent to the VLR/SGSN. The authentication and key agreement procedure is performed according to 2G specifications, i.e. using RAND in the request and SRES in the response. In the UICC only the SIM application is active.

This scenario is marked with H in figure 2.

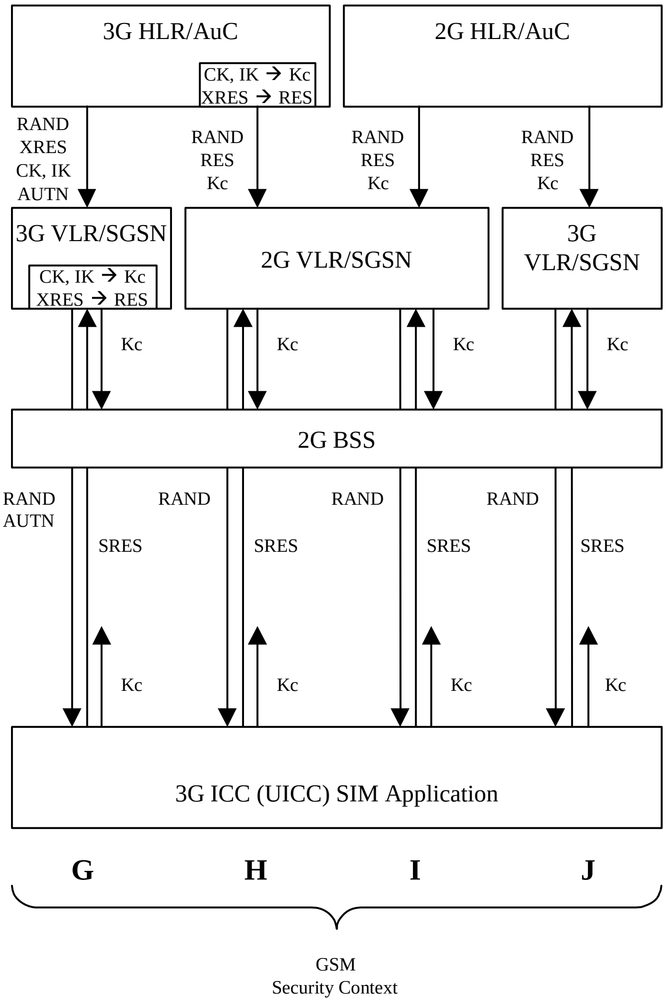

3G HLR/AuC
CK, IK → Kc
XRES → RES
2G HLR/AuC
RAND
XRES
CK, IK
AUTN
RAND
RES
Kc
RAND
RES
Kc
RAND
RES
Kc
3G VLR/SGSN
CK, IK → Kc
XRES → RES
2G VLR/SGSN
3G
VLR/SGSN
Kc
Kc
Kc
Kc
2G BSS
RAND
AUTN
RAND
RAND
RAND
SRES
SRES
SRES
SRES
Kc
Kc
Kc
Kc
3G ICC (UICC) SIM Application
G
H
I
J
GSM
Security Context

Figure 2: Possible interworking scenarios of a 2G ME and UICC with different network environments

Case 6: ME, BSS and HLR/AuC are 2G, ICC and VLR/SGSN are 3G. This applies when e.g. in the start-up phase of a 3G network a UICC (with SIM application) is introduced as the first migration step, while the rest of the network is still 2G and a user roams into another starting 3G network with 3G VLR/SGSN and 2G BSS technology.

Since the 3G VLR/SGSN is transparent for 2G AKA and the SIM application is active on the UICC, the system works entirely like 2G.

This scenario is marked with J in figure 2.

Case 8: ME, BSS, VLR/SGSN and HLR/AuC are 2G, only the ICC is a 3G UICC. This applies when in the start-up phase of a 3G network a UICC (with SIM application) is introduced as the first migration step, while the rest of the network is still 2G. With the UICC virtually being a SIM, this case can be seen as entirely 2G.

This scenario is marked with I in figure 2.

6.2.2 2G ME of R99 or Rel-4 with USIM support or of Rel-5

When the ME is 2G of R99 or Rel-4 with USIM support or of Rel-5 and the ICC is 3G (i.e. it is a UICC), a SIM application on the UICC is not necessary since the ME can interwork with the USIM. It also supports 3G AKA. Again eight different combinations of the remaining three network components are existing. They are given in the following table:

Case	ICC	ME	BSS	VLR/SGSN	HLR/AuC	Service	Figure 3
1	3G	2G (with USIM support)	3G	3G	3G	no	
2			2G	3G	3G	yes 1)	B'
3			3G	2G	3G	no	
4			2G	2G	3G	yes 2)	C'
5			3G	3G	2G	no	
6			2G	3G	2G	yes 2)	E'
7			3G	2G	2G	no	
8			2G	2G	2G	yes 2)	D'
Note: 1) requires service n° 27 supported by the USIM 2) requires services n° 27 and n° 38 supported by the USIM							

Cases 1, 3, 5, 7: A 2G ME cannot interwork with a 3G BSS. Further, in cases 3 and 7, a 3G BSS does not work in combination with a 2G VLR/SGSN. No service in these cases.

Case 2: All system elements are 3G, except for the terminal and the radio interface, which are 2G. This applies when a 3G UICC in a 2G ME roams into a 2G radio access network, which is connected to a 3G VLR/SGSN (e.g. when in the start phase of a 3G network not yet all existing 2G BSS are replaced by 3G technology, while the VLR/SGSN is already 3G).

The 2G ME with USIM support or the Rel-5 2G ME and the 2G BSS are transparent for 3G authentication parameters. To derive the ciphering key Kc for the 2G BSS, the 3G VLR/SGSN and the 3G ICC have to compute Kc from CK, IK with conversion function c3 and send it to the BSS and to the ME. Despite a 2G radio access network is involved, 3G security context is established.

The USIM receives parameters RAND and AUTN and calculates RES, CK and IK. If service n° 27 is available, Kc is generated by conversion function c3 and additionally included in the response. The keys CK and IK are not needed in this security scenario and can be discarded by the ME. If the USIM does not support service n° 27, network access is not possible.

This scenario is marked with B' in figure 3.

Case 4: ICC and HLR/AuC are 3G, ME, BSS and VLR/SGSN are 2G. This applies when a 3G UICC in a 2G ME roams into a 2G network - a very common case as networks will introduce 3G technology at different times or not at all.

Upon request by a 2G VLR/SGSN the 3G HLR/AuC produces 2G triplets RAND, RES, Kc out of 3G quintets RAND, XRES, CK, IK, AUTN. It therefore applies conversion function c2 to generate RES from XRES and conversion function c3 to generate Kc from CK and IK. RAND is left unchanged and AUTN is discarded. The 2G triplet is then sent to the VLR/SGSN. Between the VLR/SGSN and the USIM 2G AKA is executed, i.e. using RAND in the request and SRES in the response.

To handle 2G AKA, the USIM must be capable to accept a request with RAND and return a response with SRES and Kc. The support of the virtual 2G mode is indicated by service n° 38 in the USIM Service Table. Since a 2G BSS is involved, service n° 27 is also necessary. In case the USIM does not support services n° 27 and n° 38, network access is not possible.

This scenario is marked with C' in figure 3.

Case 6: All system elements are 2G, except for the ICC and the VLR/SGSN, which are 3G. It is possible to keep a 3G subscription in a 2G HLR/AuC, however on request by a 3G VLR/SGSN this can only deliver 2G triplets RAND, RES and Kc. The 3G VLR/SGSN is backward compatible and behaves like a 2G VLR/SGSN: Between the VLR/SGSN and the USIM 2G AKA is executed, i.e. using RAND in the request and SRES in the response.

To handle 2G AKA, the USIM must be capable to accept a request with RAND and return a response with SRES and Kc. The support of the virtual 2G mode is indicated by service n° 38 in the USIM Service Table. Since a 2G BSS is involved, service n° 27 is also necessary. In case the USIM does not support services n° 27 and n° 38, network access is not possible.

This scenario is marked with E' in figure 3.

Case 8: ICC is 3G, ME, BSS, VLR/SGSN and HLR/AuC are 2G. The situation is actually very similar to case 4, but here the 2G HLR/AuC is delivering the necessary 2G triplets directly.

Again this mixed network environment requires the virtual 2G mode in the USIM, indicated by service n° 38. As a 2G BSS is involved, service n° 27 is also necessary. If the USIM does not support services n° 27 and n° 38, network access is not possible.

This scenario is marked with D' in figure 3.

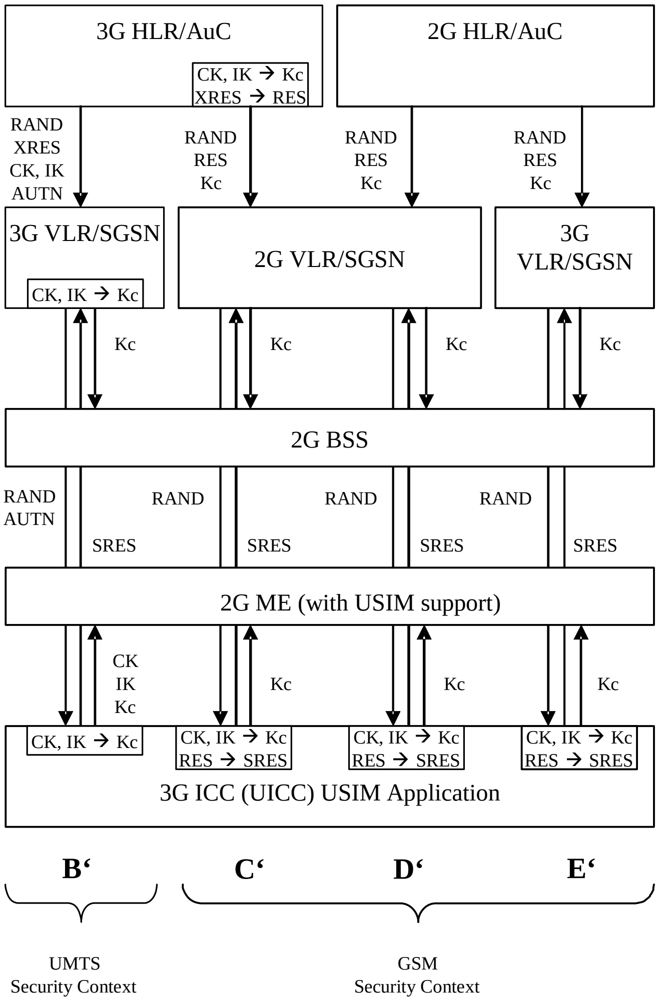

3G HLR/AuC
CK, IK → Kc
XRES → RES
2G HLR/AuC
RAND
XRES
CK, IK
AUTN
RAND
RES
Kc
RAND
RES
Kc
RAND
RES
Kc
3G VLR/SGSN
CK, IK → Kc
2G VLR/SGSN
3G
VLR/SGSN
Kc
Kc
Kc
Kc
2G BSS
RAND
AUTN
RAND
SRES
RAND
SRES
RAND
SRES
SRES
2G ME (with USIM support)
CK
IK
Kc
Kc
Kc
Kc
CK, IK → Kc
CK, IK → Kc
RES → SRES
CK, IK → Kc
RES → SRES
CK, IK → Kc
RES → SRES
3G ICC (UICC) USIM Application
B'
C'
D'
E'
UMTS
Security Context
GSM
Security Context

Figure 3: Possible interworking scenarios of a 2G ME and UICC with different network environments

6.3 With 3G ME and SIM

This combination is depending on the actual 3GPP release the terminal is compliant to.

6.3.1 3G ME of R99 or Rel-4

Any 3G ME, not only if it is a 2G/3G dual mode ME, is required to work with a 2G SIM. Again eight different combinations of the remaining three network components are existing. These can be reduced to four, as the technology of the HLR/AuC is not relevant: A 2G HLR/AuC will always deliver 2G triplets and a 3G HLR/AuC will do the same because a 2G subscriber (his IMSI is linked to 2G functionality) is involved. The remaining four cases are given in the following table:

Case	ICC	ME	BSS	VLR/SGSN	HLR/AuC	Service	Figure 3
1	2G	3G	3G	3G	2G or 3G	yes	K
2			2G	3G		yes 1)	L
3			3G	2G		no	
4			2G	2G		yes 1)	M
Note: 1) 2G/3G dual mode ME required							

Case 1: ME, BSS and VLR/SGSN are 3G, the ICC is 2G (i.e. a SIM). This applies when e.g. a 2G subscriber with a 3G ME roams in a 3G network.

Any HLR/ AuC will deliver triplets to the 3G VLR/SGSN. The 3G BSS requires CK and IK, so the VLR/SGSN applies conversion function c3 to generate them from Kc. The SIM can only perform 2G AKA and returns SRES, Kc to the ME which also applies c3 to generate CK, IK. Despite the usage of CK and IK, security is based on Kc, i.e. 2G security context is established.

This scenario is marked with K in figure 3.

Case 2: ME and VLR/SGSN are 3G, ICC and BSS are 2G. This applies when e.g. a 2G subscriber with 3G ME roams in a 3G network with 2G BSS.

The situation is like in case 1, except that with a 2G BSS there is no need to derive CK, IK from Kc in the VLR/SGSN and in the ME. Both, the 3G VLR/SGSN and a 2G/3G dual mode ME can work with 2G AKA. No service with a 3G single mode ME.

This scenario is marked with L in figure 3.

Case 3: ME and BSS are 3G, ICC and VLR/SGSN are 2G. As a 2G VLR/SGSN and a 3G BSS are not compatible, this theoretical combination cannot exist. No service in this case.

Case 4: ICC, BSS and VLR/SGSN are 2G, the ME is 3G. This applies when e.g. a 2G subscriber with a 3G ME roams in a 2G network.

2G AKA is performed just like in a plain 2G situation. A 2G/3G dual mode ME is transparent for 2G AKA. No service with a 3G single mode ME.

This scenario is marked with M in figure 3.

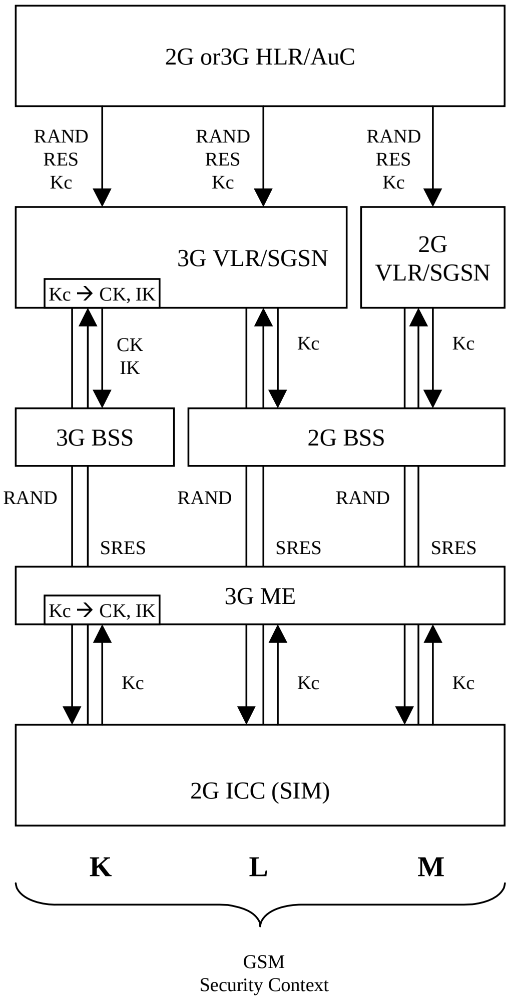

2G or3G HLR/AuC
RAND
RES
Kc
RAND
RES
Kc
RAND
RES
Kc
3G VLR/SGSN
Kc → CK, IK
2G
VLR/SGSN
CK
IK
Kc
Kc
3G BSS
2G BSS
RAND
RAND
RAND
SRES
SRES
SRES
3G ME
Kc → CK, IK
Kc
Kc
Kc
2G ICC (SIM)
K
L
M
GSM
Security Context

Figure 4: Possible interworking scenarios of a 3G ME and SIM with different network environments

6.3.2 3G ME of Rel-5

For a 3G ME of Rel-5 support of the 2G SIM is only optional. If this option is taken (strongly recommended as there are huge quantities of legacy 2G SIMs in almost all major markets), there is no difference to section 6.3.1. Otherwise this combination does not work.

6.4 With 2G ME and SIM

This combination is depending on the actual 3GPP release the terminal is compliant to.

6.4.1 2G ME of Rel-4 (or earlier)

This ME/ICC combination results more or less in the "old" 2G case. Like in section 6.3 the HLR/AuC is not relevant, so theoretically 4 cases remain as given in the following table:

Case	ICC	ME	BSS	VLR/SGSN	HLR/AuC	Service	Figure 4
1	2G	2G	3G	3G	2G or 3G	no	
2			2G	3G		yes	N
3			3G	2G		no	
4			2G	2G		yes	O

Case 1: A 2G ME cannot interwork with a 3G BSS. No service in this case.

Case 2: The VLR/SGSN is 3G, the HLR is 2G or 3G and the rest is 2G. The VLR/SGSN is backwards compatible and enters 2G mode. 2G AKA is executed.

This scenario is marked with N in figure 4.

Case 3: A 2G ME cannot interwork with a 3G BSS. Further, a 3G BSS does not work in combination with a 2G VLR/SGSN. No service in this case.

Case 4: The HLR is 2G or 3G and the rest is 2G. There is no difference to the well-known classic 2G case. 2G AKA is executed.

This scenario is marked with O in figure 4.

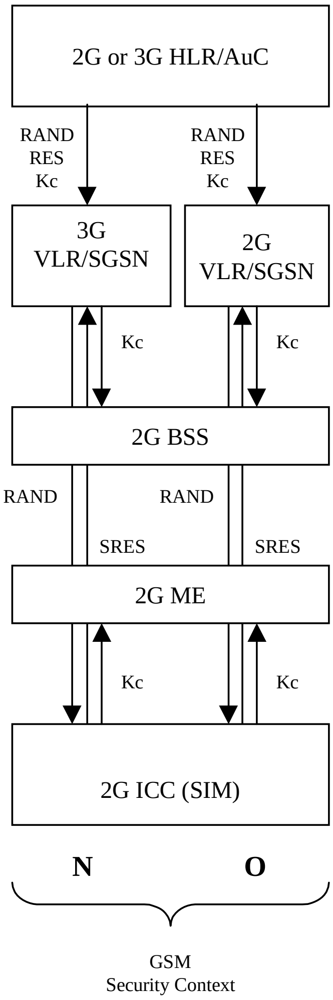

2G or 3G HLR/AuC
RAND
RES
Kc
RAND
RES
Kc
3G
VLR/SGSN
2G
VLR/SGSN
Kc
Kc
2G BSS
RAND
RAND
SRES
SRES
2G ME
Kc
Kc
2G ICC (SIM)
N
O
GSM
Security Context

Figure 5: Possible interworking scenarios of a 2G ME and SIM with different network environments

6.4.2 2G ME of Rel-5

For a 2G ME of Rel-5 support of the 2G SIM is only optional. If this option is taken (strongly recommended as there are huge quantities of legacy 2G SIMs in almost all major markets), there is no difference to section 6.4.1. Otherwise this combination does not work.

7 Interworking between a SIM application and a USIM application on a UICC

A SIM application and a USIM application which are implemented together on a single UICC can never be active at the same time. Neither can they be switched from one to the other. Their activity solely depends on the type of ME in which they are inserted: A 2G ME will always activate the SIM application, while a 3G ME only uses the USIM application. Hence a direct way of interworking does not exist.

However, both applications may share certain elements, either to enable an intended basic subscription mode of the UICC (single or double subscription) or to optimise memory consumption, but still both applications have to be virtually independent from a functional point of view. This means that a 2G ME can interwork with the SIM application without any influence from the USIM, while a 3G ME finds all the mandatory characteristics of the USIM application. Naturally, independence ends if one application changes shared data which is later accessed by the other application because the UICC was inserted into another type of ME. This has to be taken into account.

The following sections describe the possible options.

7.1 IMSI, secret key and authentication algorithm

In the HLR/AuC, a single subscription is identified by a particular IMSI, which is connected to a particular secret key (given by "Ki" for 2G, "K" for 3G) and to one type of authentication algorithm ("A3/A8" for 2G, "f1-f5" for 3G). At no time, a single IMSI may be connected to more than one secret key or algorithm. This is valid for both 2G and 3G contexts. Further, it applies that

- Length and Format ($IMSI_{2G}$) = Length and Format ($IMSI_{3G}$)
- Length (Ki) = Length (K)
- 2G-Type Algorithm = Part of 3G Algorithm + Conversion Functions c2, c3

For the third "equation" see Annex B2 or 3G TS 31.102 [2] and 3G TS 33.102 [6]. This 2G behaviour of the 3G algorithm is the same as the virtual 2G mode described in section 5.1. If it is always active, e.g. in a SIM application or in a 2G HLR/AuC, it shall in the following be called a fixed virtual 2G mode. Then, in fact, it is a 2G algorithm.

There are three possible options for the UICC:

1. **Separate IMSI & Separate Secret Key:** This case applies if the network operator - for some reason - wants to administrate the 2G and the 3G subscription, i.e. the usage of a 2G or 3G ME, fully independent. The two subscriptions can be maintained in either in a single 2G or 3G HLR/AuC or in different dedicated 2G and 3G HLR/AuCs. Then USIM and SIM applications also have to keep separate IMSIs, i.e. $IMSI_{3G} \neq IMSI_{2G}$. The secret keys have to be different as well, i.e. $K \neq Ki$. Of course, the algorithms in the UICC have to correspond to the algorithms associated with the IMSIs in the HLR/AuCs. The USIM application needs a 3G algorithm, while for the SIM application it can either be
    - a 2G algorithm on its own or
    - a 3G algorithm in fixed virtual 2G mode. In that case the UICC needs to implement a 3G algorithm only, which from the SIM application is executed in 2G mode. The HLR/AuC must support this option accordingly.
2. **Separate IMSI & Shared Secret Key:** From a functional point of view, this option is identical to option 1, except that the UICC saves 128 bits for the storage of a second secret key. On the other hand, the deliberate assignment of the same secret key to two different IMSIs would require particular solutions during secret key generation and pre-personalization.
3. **Shared IMSI & Shared Secret Key:** This case applies if the network operator wants to have one single subscription for a user, independent of the usage of a 2G or 3G ME. Consequently the UICC has to carry the same identification details, i.e. IMSI and secret key, in both SIM and USIM applications. On the network side there is a single entry consisting of one IMSI and one secret key in either a 2G or a 3G HLR/AuC, i.e. $IMSI_{3G}$ = $IMSI_{2G}$ and K = Ki. In a 2G HLR the algorithm has to be a 3G-type in fixed virtual 2G mode (a 3G algorithm does not fit into a 2G HLR and a 2G algorithm does not fit with the USIM application on the UICC) while in a

3G HLR the algorithm is a 3G-type. On the UICC side there is not much choice: The USIM application essentially needs a 3G algorithm while for the SIM application it can only be a 3G-algorithm in (fixed) 2G mode as there is no 2G-type in the network. Again this has the advantage of having only one shared 3G algorithm on the UICC, which from the SIM application is executed in 2G mode.

The fourth theoretical combination, namely shared IMSI & separate secret keys, is not a valid option as a single IMSI cannot be associated with more than one secret key simultaneously.

7.2 File mapping

When comparing the file structure of a SIM in TS 11.11 [7] / TS 51.011 [8] with that of a USIM in 3G TS 31.102 [2] it strikes that many not only have the same name and file identifier (although under different DFs) but are entirely equal by size and content parameters. This generally allows for memory efficient implementation of a SIM together with a USIM as these files can be shared by both applications, i.e. necessary storage capacity is only required once. Further, shared files speed up the pre-personalization process as they save valuable programming time.

Therefore files should be mapped as far as possible, i.e. in all cases where basic properties are equal and identical contents do not conflict with the access by either a 2G or a 3G ME or with intended subscription differences when separate IMSIs are used (cases 1 or 2 in section 7.1). Mapping is not possible, when the content is clearly subscription dependent like in case of IMSI, Kc, KcGPRS or MSISDN in a double subscription UICC.

Annex C gives an overview on the SIM and USIM files that potentially can be mapped. A case by case decision should be conducted by the network operator / card manufacturer for each UICC implementation. Caution: It should be noted that file identifiers may differ between the SIM and USIM applications, while all other file properties are exactly the same, e.g. for EF_{EXT4}.

7.3 Access conditions

If a EF or DF is accessible in both 2G and 3G operation modes (e.g. in the MF: EF-PL in the UICC can be identical to EF-ELP in the SIM), then independent 2G and 3G access conditions may be defined for the file. The UICC does not check the consistency of the access conditions in both modes.

Therefore it is possible that the same EF or DF has different security attributes in 2G and 3G operation mode. It is the responsibility of the network operator and the card manufacturer to ensure at the personalisation stage that the security attributes for 2G and 3G session are the same, if necessary.

7.4 Secret codes

In 3G mode, 8 Application PINs with global key references are available and the UICC also supports up to 8 Local PINs with specific key references. Local PINs can only be used within an ADF. Further, up to 10 administrative PINs can be defined. A replacement PIN, called Universal PIN, may also exist.

In 2G mode, only CHV1 and CHV2 are available. They apply to files in DF-GSM and DF-TELECOM. Additionally, up to 11 administrative PINs can be defined.

Mapping of PINs between 2G and 3G operation modes, so that activation, deactivation or changing of a PIN in one operation mode has the same effect in the other operation mode, follow the following principles:

- **Mapping of CHV1**

  CHV1 in the SIM application can be mapped to any USIM application PIN with a global key reference (or to the Universal PIN, if the UICC is multi-verification capable), but to only one at a time.

  When the UICC is single-verification capable, CHV1can only be mapped to a USIM application PIN. Then, if the USIM application PIN is disabled, the CHV1 is also disabled and vice versa. See also Annex D.1.

  When the UICC is multi-verification capable, different mappings of CHV1 are possible, depending on the standards release to which the UICC is compliant to:

  - **Static mapping:** CHV1 is always mapped to a USIM application PIN. If the USIM application PIN is disabled and replaced by the Universal PIN, then also CHV1is disabled. Thus when using the USIM, the user will have to verify the Universal PIN. When using the SIM, there will be no verification. Therefore, in this case the SIM and the USIM behave differently regarding the PIN/CHV1 verification from the user's point of view. Static mapping is only possible for R99 and REL-4 UICCs. See also Annex D.2.

- **Dynamic mapping:** CHV1 is mapped to the USIM application PIN but the mapping can change to the Universal PIN. When the USIM application PIN is enabled, then CHV1 is also enabled. If the USIM application PIN is disabled and not replaced, then CHV1 is disabled. If the USIM application PIN is disabled and replaced by the Universal PIN, then CHV1 is mapped to the Universal PIN, i.e. the mapping changes from the application PIN to its replacement. In this case the behaviour of the SIM and the USIM is exactly the same regarding the PIN/CHV1 verification from the user's point of view. Dynamic mapping is possible for UICCs of any 3G release. See also Annex D.3.

- **Mapping of CHV2**

  CHV2 in the SIM application can be mapped to the corresponding local key reference belonging to the USIM application to which the CHV1 is mapped. In the 2G operation mode, this PIN is considered to be global, in the 3G operation mode, it is seen as a being local. If mapped, then, with respect to the requirement in TS 11.11 [7] / TS 51.011 [8] for CHV2, this PIN cannot be disabled in either operation mode. The UICC will return an appropriate error condition in that case.

- **Mapping of Local PINs**

  A SIM does not support Local PINs, hence there is no correspondence in 2G operation mode. Local PINs cannot be mapped.

- **Mapping of administrative PINs**

  The mapping of administrative PINs between the 2G and 3G operation modes is fully under the discretion of each network operator and card manufacturer.

7.5 Activation of 2G and 3G operation modes

After a cold reset has been performed (i.e. during UICC activation), the ATR sent by the UICC is compliant to 3G TS 31.101 [1]. No particular operation mode is active at this stage. The selection and activation of either 2G operation mode (i.e. the SIM application) or 3G operation mode (i.e. the USIM application), is implicitly done by the ME when sending the first command. The following table describes the different possible cases.

UICC / ME Combination	Class Byte of First Command	Resulting UICC Operation Mode	Remark

UICC with or without a SIM application in a 3G or 2G/3G dual mode ME or in a 2G ME of R99 or Rel-4 with USIM support or in a 2G ME of Rel-5	'0X' or '8X'	3G	The USIM application rejects commands with class byte = 'A0'. First command right after ATR can be SELECT or STATUS.
UICC with a SIM application in a 2G ME of Rel-4 or earlier without USIM support	'A0'	2G	The SIM application rejects commands with class byte = '0X' or '8X'. First command right after ATR can be SELECT, STATUS or GET RESPONSE.
UICC without a SIM application in a 2G ME of Rel-4 or earlier without USIM support	'A0'	No operation!	All further commands with class byte = 'A0' will be rejected.

A 3G or 2G/3G dual mode ME or a 2G ME of R99 or Rel-4 with USIM support or a 2G ME of Rel-5 will only send commands with class byte = '0X' or '8X'. A 2G ME of Rel-4 (or earlier) without USIM support will only send commands with class byte = 'A0'. The operation mode selection takes place regardless of the result of the command (i.e. if it was successful or not).

7.6 Selection of cyclic files

As the SIM application and the USIM application are based on individual specifications, a particular difference applies for the selection of cyclic files.

For the SIM, TS 11.11 [7] / TS 51.011 [8] specifies that "After selection of a cyclic file (for either operation), the record pointer shall address the record updated or increased last.", whereas for the USIM it is required in 3G TS 31.101 [1] that "After a successful selection the record pointer is undefined.". In the latter case, the record pointer is set implicitly by the subsequent access command.

Therefore, in the case of a selection of cyclic files, the UICC will behave corresponding to its current operation mode, i.e. comply to 2G requirements when the SIM application is active and to 3G requirements when the USIM application is active.

A 3G ME shall handle this situation accordingly, i.e. depending on whether a SIM or a UICC is inserted.

7.7 Enabling/disabling procedures for dialling numbers

Enabling/disabling procedures of restricted dialling numbers services (e.g. FDN or BDN) are different between SIM and USIM. In fact, simply mapping the files associated with such services between the SIM and USIM will not ensure consistent behaviour in GSM and 3G modes, and can actually allow the user to bypass the associated security by switching the UICC between a 2G and a 3G terminal. Therefore, if a dialling number file (e.g. EF_{FDN} or EF_{BDN}) is mapped between a SIM and a USIM, the corresponding enabling/disabling procedures should also be linked.

This means that the enabling/disabling of a restricted dialling numbers service in one mode (SIM or USIM) is reflected in the other mode (respectively USIM or SIM); i.e. any modification of the activation status of such service (e.g. FDN or BDN) for the USIM in EF_{EST} should affect the validation status of the file associated with this service (e.g. EF_{ADN} or EF_{BDN} respectively) for the SIM accordingly, and vice-versa.

The linking mechanism can only apply if the initial conditions are consistent for interworking, i.e. if the associated service (e.g. FDN or BDN) is available in the USIM Service Table (EF_{UST}) and allocated and activated in the SIM Service Table (EF_{SST})..

NOTE: If the status of a restricted dialling numbers service is modified Over The Air in the SIM or USIM Service Table (EF_{SST} or EF_{UST}), the linking mechanism may not be able to maintain the synchronization of the service status between SIM and USIM.

8 Interworking between USIM applications on a UICC

If a UICC contains more than one USIM application, these are normally related to separate subscriptions, either from the same or from different network operators. In that case IMSIs and secret keys are different and cannot be shared. The authentication algorithm may be shared if the nature of the subscriptions does not require different algorithms.

Concerning the mapping of files between multiple USIMs, only the following guidelines can be given:

- If the UICC is intended to be used by a single user, all user relevant files (that can be updated by the user) could be mapped. The phonebook will preferably be located under DF TELECOM, to enable global access from all applications. In a multi-user model, user relevant files should not be mapped and a specific phonebook will be under each DF USIM.
- All directly subscription relevant files (like Kc or MSISDN) or those needed to differentiate the subscriptions should not be mapped.
- All other files: Mapping depends on conditions of use in a multi-subscription environment.

If a SIM application is existing in addition to multiple USIM applications, mapping can be done according to section 7 and Annex C with one of the USIM applications.

As it is not possible to cover all specific situations that might require multiple USIMs on a UICC, such design decisions should be taken on a case by case basis by considering each data field and its possible use.

9 SIM and UICC Interworking on the Card/Terminal Interface

The SIM specification in TS 11.11 [7] / TS 51.011 [8] and the UICC/USIM specification in TS 31.101 [1] contain some different requirements affecting the physical card/terminal interface.

As the interface behaviour needs to be independent of the applications supported, a UICC holding both a SIM and a USIM application, or a terminal accepting both legacy SIM and UICCs, satisfies all the requirements from all the specifications they are complying with.

TS 11.11 [7] / TS 51.011 [8] and TS 31.101 [1] contain no contradictory requirements, but the strongest requirements from these two sets of specifications need to apply.

In particular, such cards and terminals are ready to receive data 12 etus after they begin sending their last outgoing character (to comply with the SIM specification) but do not start transmitting outgoing data less than 16 etus after they begin receiving the last incoming character (to comply with the USIM specification).

This implies that a 12 etu reception turnaround guardtime is supported at all speeds supported, as indicated by the card in the ATR,

The highest speed supported is compliant with the requirements of TS 31.101 [1].

The ATR of a 31.101 [1] compliant UICC always includes T=15 parameters. This applies for a UICC that only contains a USIM application (TS 31.102 [2]), it applies for a UICC that only contains a SIM application (TS 51.011 [8]) and it also applies for a UICC that contains both a USIM and a SIM application.

An ATR of a SIM as defined in TS 11.11 [7] may contain these T=15 parameters even though these parameters are not requested by TS 11.11 [7].

Annex A:
Interworking table

The following table lists the complete set of interworking scenarios introduced by the two possible types of generation (2G or 3G) with each of the main network elements involved in authentication and key agreement. These are ICC, ME, BSS, VLR/SGSN and HLR/AuC.

In each case the function of the network elements is commented when the behaviour is particular for the case. No comment means that the behaviour is not special for the purpose of interworking. If a case was identified as not functional, i.e. interworking fails somewhere through the transmission chain, this is indicated by grey background. A more detailed explanation of each case can be found in section 6 of this document. The character in the last column refers to figures 1 to 4 in section 6.

ICC	ME	BSS	VLR	AUC	ICC	ME	BSS	VLR/SGSN	HLR/AuC	Security Con	Figure 1-4
2	2 5)	2	2	2						2G	O
2	2 5)	2	2	3					3G HLR/AC generates 2G triplets for 2G IMSI	2G	O
2	2 5)	2	3	2				3G VLR/SGSN transparent for 2G AKA		2G	N
2	2 5)	2	3	3					3G HLR/AC generates 2G triplets for 2G IMSI	2G	N
2	2	3	2	2			3G BSS incompatible with 2G ME and 2G VLR/SGSN				
2	2	3	2	3			3G BSS incompatible with 2G ME and 2G VLR/SGSN				
2	2	3	3	2			3G BSS incompatible with 2G ME				
2	2	3	3	3			3G BSS incompatible with 2G ME				
2	3 6)	2	2	2		3G ME transparent for 2G AKA 2)				2G	M
2	3 6)	2	2	3		3G ME transparent for 2G AKA 2)			3G HLR/AC generates 2G triplets for 2G IMSI	2G	M
2	3 6)	2	3	2		3G ME transparent for 2G AKA 2)		3G VLR/SGSN transparent for 2G AKA		2G	L
2	3 6)	2	3	3		3G ME transparent for 2G AKA 2)		3G VLR/SGSN transparent for 2G AKA	3G HLR/AC generates 2G triplets for 2G IMSI	2G	L
2	3	3	2	2			3G BSS incompatible with 2G VLR/SGSN				
2	3	3	2	3			3G BSS incompatible with 2G VLR/SGSN				
2	3 6)	3	3	2		3G ME transparent for 2G AKA, generates CK,	3G BSS transparent for 2G AKA	3G VLR/SGSN transparent for 2G AKA, generates CK,		2G	K

2	3 6)	3	3	3		3G ME transparent for 2G AKA, generates CK,	3G BSS transparent for 2G AKA	3G VLR/SGSN transparent for 2G AKA, generates CK,	3G HLR/AC generates 2G triplets for 2G IMSI	2G	K
3	2 7)	2	2	2							D'
3	2 7)	2	2	3					3G HLR/AC generates Kc from CK, IK and RES from XRES		C'
3	2 7)	2	3	2				3G VLR/SGSN transparent for 2G AKA			E'
3	2 7)	2	3	3				3G VLR/SGSN generates Kc from CK, IK			B'
3	2	3	2	2			3G BSS incompatible with 2G ME				
3	2	3	2	3			3G BSS incompatible with 2G ME				
3	2	3	3	2			3G BSS incompatible with 2G ME				
3	2	3	3	3			3G BSS incompatible with 2G ME				
3	3	2	2	2	2G mode 4)	3G ME transparent for 2G AKA 2)				2G	D
3	3	2	2	3	2G mode 4)	3G ME transparent for 2G AKA 2)			3G HLR/AC generates Kc from CK, IK and RES from XRES	2G	C
3	3	2	3	2	2G mode 4)	3G ME transparent for 2G AKA 2)		3G VLR/SGSN transparent for 2G AKA		2G	E
3	3	2	3	3	3G + Kc mode 3)	2)		3G VLR/SGSN generates Kc from CK, IK		3G	B
3	3	3	2	2			3G BSS incompatible with 2G VLR/SGSN				
3	3	3	2	3			3G BSS incompatible with 2G VLR/SGSN				
3	3	3	3	2		3G ME with UICC shall not execute 2G AKA when attached to a 3G BSS					F

3	3	3	3	3						3G	A
3 1)	2 8)	2	2	2	SIM appl. active					2G	I
3 1)	2 8)	2	2	3	SIM appl. active				3G HLR/AC generates Kc from CK, IK and RES from XRES	2G	H
3 1)	2 8)	2	3	2	SIM appl. active			3G VLR/SGSN transparent for 2G AKA		2G	J
3 1)	2 8)	2	3	3	SIM appl. active			3G VLR/SGSN generates Kc from CK, IK and RES from XRES		2G	G
3 1)	2 8)	3	2	2			3G BSS incompatible with 2G ME and 2G VLR/SGSN				
3 1)	2 8)	3	2	3			3G BSS incompatible with 2G ME and 2G VLR/SGSN				
3 1)	2 8)	3	3	2			3G BSS incompatible with 2G ME				
3 1)	2 8)	3	3	3			3G BSS incompatible with 2G ME				

NOTE: 1) UICC with SIM application
NOTE: 2) 2G/3G dual mode ME required, no service otherwise
NOTE: 3) Support of service n° 27 required in the USIM, no service otherwise
NOTE: 4) Support of services n° 27 and n° 38 required in the USIM, no service otherwise
NOTE: 5) 2G ME of Rel-4 (or earlier) or of Rel-5 with (optional) SIM support
NOTE: 6) 3G ME of Rel-4 (or earlier) or of Rel-5 with (optional) SIM support
NOTE: 7) 2G ME of R99 or Rel-4 with USIM support or of Rel-5
NOTE: 8) 2G ME of Rel-4 (or earlier) without USIM support

Annex B: Features for security interworking

The following sections summarise the features defined to convert security parameters between 2G and 3G or vice versa. For more information see 3G TS 33.102 [6].

B.1 Conversion functions

Conversion function c1 converts a 128 bit 3G random challenge into a 128 bit 2G random challenge. Both values have the same format, i.e. they are equal.

c1: $RAND_{2G} = RAND_{3G}$

Conversion function c2 converts a 3G expected authentication response XRES into a 2G expected authentication response RES (in the AuC or the VLR/SGSN) or a 3G authentication response RES into a 2G authentication response SRES (in the USIM).

c2: $RES_{2G} = XRES_{3G,\,1}$ [xor $XRES_{3G,\,2}$ [xor $XRES_{3G,\,3}$ [xor $XRES_{3G,\,4}$]]]

$SRES_{2G} = RES_{3G,\,1}$ [xor $RES_{3G,\,2}$ [xor $RES_{3G,\,3}$ [xor $RES_{3G,\,4}$]]]

where $RES_{3G,\,i}$ or $XRES_{3G,\,i}$ are 32 bits long and $(X)RES_{3G} = (X)RES_{3G,\,1}$ [|| $(X)RES_{3G,\,2}$ [|| $(X)RES_{3G,\,3}$ [|| $(X)RES_{3G,\,4}$]]] depending on the length of $(X)RES_{3G}$ (a multiple of 32 bit or else be padded with "0"). In the USIM, conversion function c2 must be supported in connection with conversion function c3 and the ability to execute a "reduced" 3G algorithm. This optional service is indicated by service n° 38 in the USIM Service Table.

Conversion function c3 converts the 128 bit 3G ciphering and integrity protection keys CK and IK into the 64 bit 2G ciphering key Kc. This function is applied in the AuC or VLR/SGSN and in the USIM.

c3: $Kc = CK_1$ xor CK_2 xor IK_1 xor IK_2

where CK_i and IK_i are both 64 bits long and $CK = CK_1 \| CK_2$ and $IK = IK_1 \| IK_2$. In the USIM, the optional support of conversion function c3 is indicated by service n° 27 in the USIM Service Table.

Conversion function c4 converts a 64 bit 2G Kc into a 128 bit 3G CK. This function is applied in the ME and in the VLR/SGSN.

c4: $CK = Kc \| Kc$

Conversion function c5 converts a 64 bit 2G Kc into a 128 bit 3G IK. This function is applied in the ME and in the VLR/SGSN.

c5: $IK = (Kc_1 \text{ xor } Kc_2) \| Kc \| (Kc_1 \text{ xor } Kc_2)$

where Kc_i are both 32 bits long and $Kc = Kc_1 \| Kc_2$.

B.2 3G algorithm execution modes

The 3G algorithm in the USIM consists of five sub-functions that have to be executed in order to verify the received data and generate the necessary responses. For more information see 3G TS 31.102 [2] and 3G TS 33.102 [6].

In **normal 3G mode** the input is given by RAND and AUTN. The USIM computes

- f5 to get the anonymity key AK. AK is then used to retrieve the sequence number SQN.
- f1 to derive XMAC. XMAC is then used to verify the authenticity of the home environment.
- f2 to calculate the 3G authentication response RES

- f3 to get the 3G ciphering key CK
- f4 to get the 3G integrity protection key IK

The USIM returns RES, CK and IK.

In **3G + Kc mode** the input is also given by RAND and AUTN. The USIM computes the same sequence of functions but in the end applies conversion function c3 to generate a 2G Kc from CK and IK. The USIM returns RES, CK, IK and Kc. Kc is always returned if this mode is active in the USIM. If not needed, the ME may discard the additional Kc.

In **virtual 2G mode** the input is only given by RAND. The USIM skips functions f5 and f1 and only executes f2, f3 and f4 ("reduced" 3G algorithm). Subsequently it applies conversion function c3 to generate 2G Kc from CK, IK and conversion function c2 to generate 2G SRES from RES. The USIM returns SRES and Kc. The ME can require the USIM to operate in this mode by sending a specific command parameter. If it is not supported by the USIM, an error indication is returned.

NOTE: The 3G algorithm in 2G mode is virtually (i.e. by input and output) identical to a 2G algorithm. A UICC with USIM and SIM applications may make use of that and implement a 3G algorithm only, which from the SIM application is executed in 2G mode.

Annex C:
SIM/USIM file mapping table

The following table lists all SIM and USIM files that can be mapped in a UICC. It should be noted that most files are optional and these files are not necessarily present in the SIM or USIM application. Files not mentioned do not have a corresponding file in both applications. Mapping with multiple USIMs is not considered.

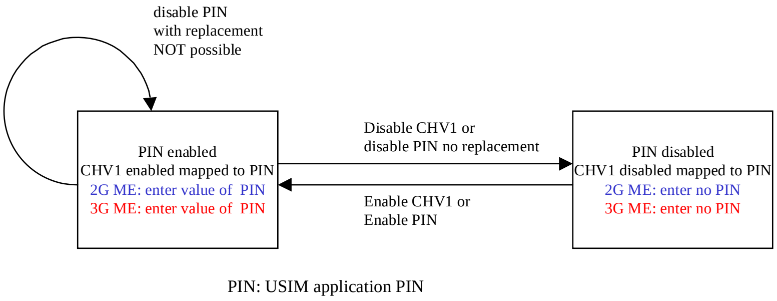
SIM Application DF / EF	USIM Application DF / EF	Mapping possible	
		single subscription UICC	**double subscription UICC**
GSM / IMSI	USIM / IMSI	yes	no
GSM / HPLMN	USIM / HPLMN	yes	yes, 1)
GSM / ACM	USIM / ACM	yes	yes, 1)
GSM / ACMmax	USIM / ACMmax	yes	yes, 1)
GSM / PUCT	USIM / PUCT	yes	yes, 1)
GSM / GID1	USIM / GID1	yes	yes, 1)
GSM / GID2	USIM / GID2	yes	yes, 1)
GSM / SPN	USIM / SPN	yes	yes, 1)
GSM / CBMI	USIM / CBMI	yes	
GSM / CBMIR	USIM / CBMIR	yes	
GSM / CBMID	USIM / CBMID	yes	yes, 1)
GSM / ACC	USIM / ACC	yes	no
GSM / FPLMN	USIM / FPLMN	yes, 7)	yes, 1)
GSM / LOCI	USIM / LOCI	yes, 8)	no
GSM / LOCIGPRS	USIM / PSLOCI	yes, 5) 8)	no
GSM / AD	USIM / AD	yes	
GSM / eMLPP	USIM / eMLPP	yes	yes, 1)
GSM / AAeM	USIM / AAeM	yes	yes, 1)
GSM / DCK	USIM / DCK	yes	yes, 1)
GSM / CNL	USIM / CNL	yes	yes, 1)
GSM / PLMNwACT	USIM / PLMNwACT	yes	
GSM / OPLMNwACT	USIM / OPLMNwACT	yes	yes, 1)
GSM / HPLMNwACT	USIM / HPLMNwACT	yes, 3)	
GSM / SUME	TELECOM / SUME	yes	
GSM / Kc	USIM / GSM / Kc	yes	no
GSM / KcGPRS	USIM / GSM / KcGPRS	yes	no
GSM / CPBCCH	USIM / GSM / CPBCCH	yes	
GSM / INVSCAN	USIM / GSM / INVSCAN	yes	yes, 1)
GSM / PNN	USIM / PNN	yes	yes, 1)
GSM / OPL	USIM / OPL	yes	yes, 1)
GSM / MBDN	USIM / MBDN	yes	no
GSM / EXT6	USIM / EXT6	yes	no
GSM / MBI	USIM / MBI	yes	no
GSM / MWIS	USIM / MWIS	yes	no
GSM / CFIS	USIM / CFIS	yes	no
GSM / EXT7	USIM / EXT7	yes	no
GSM / SPDI	USIM / SPDI	yes	yes, 1)

TELECOM / SMS	USIM / SMS	yes	
TELECOM / SMSP	USIM / SMSP	yes	yes, 1)
TELECOM / SMSS	USIM / SMSS	yes	
TELECOM / SMSR	USIM / SMSR	yes	
TELECOM / SDN	USIM / SDN	yes	yes, 1)
TELECOM / FDN	USIM / FDN	yes	
TELECOM / BDN	USIM / BDN	yes	
TELECOM / CMI	USIM / CMI	yes, 6)	
TELECOM / MSISDN	USIM / MSISDN	yes, 4)	no
TELECOM / EXT2	USIM / EXT2	yes	
TELECOM / EXT3	USIM / EXT3	yes	yes, 1)
TELECOM / EXT4	USIM / EXT4	yes, 5)	
TELECOM / ADN	... / PHONEBOOK / ADN	yes, required, 2)	
TELECOM / EXT1	... / PHONEBOOK / EXT1	yes, required, 2)	
TELECOM / ECCP	... / PHONEBOOK / CCP1	yes, required, 2)	
GSM / MEXE / all files	USIM / MEXE / all files	yes	yes, 1)
GSM / SoLSA / all files	USIM / SoLSA / all files	yes	yes, 1)
NOTE 1: No mapping, if subscription specific differences are required NOTE 2: SIM file to be mapped with related USIM file either in DF PHONEBOOK under DF USIM or in DF PHONEBOOK under DF TELECOM NOTE 3: Only if the same settings apply to 2G and 3G operation NOTE 4: No mapping of EF-MSISDN if EF-EXT1 is used in the SIM and / or EF-EXT5 is used in the USIM NOTE 5: Caution: Different file identifiers in SIM and USIM NOTE 6: No mapping if coding "FF" is used in the content NOTE 7: Mapping is possible only if the size of FPLMN is 12 bytes NOTE 8: Mapping recommended to keep LAIs / RAIsin SIM and USIM synchronised in order to avoid potential network malfunction when changing the UICC between 2G and 3G operation.			

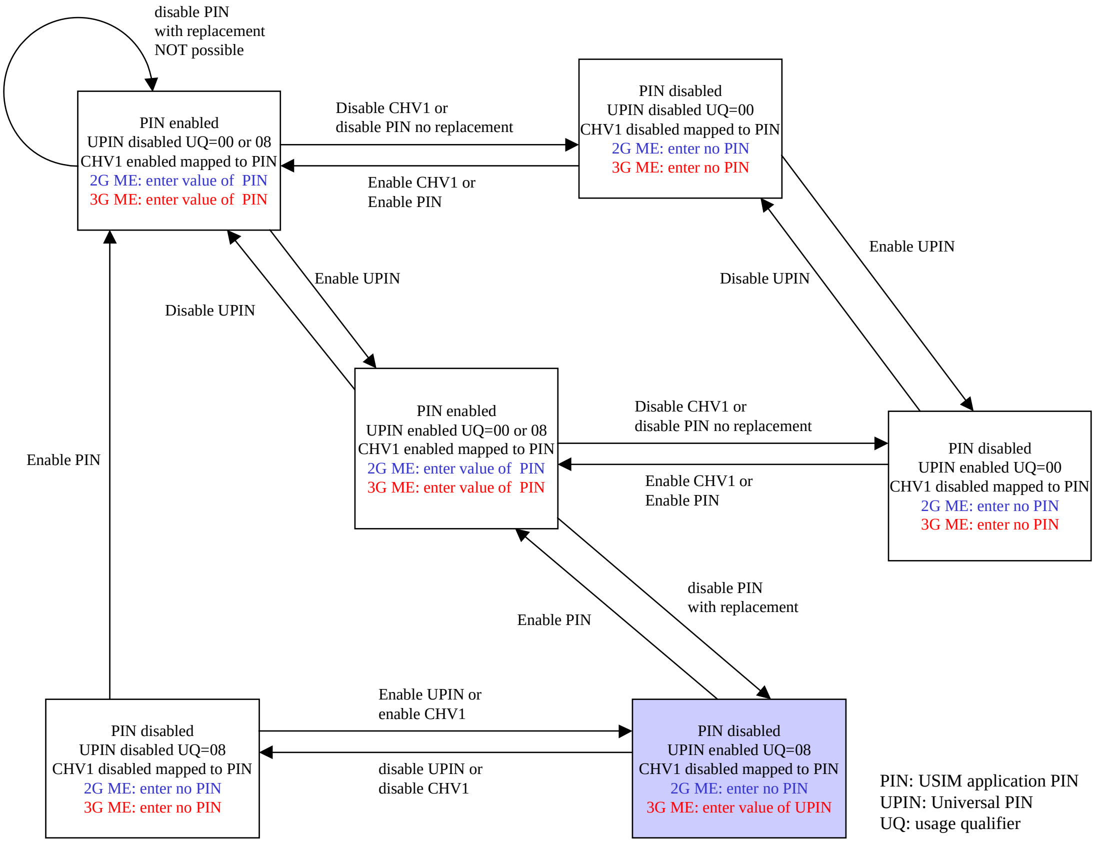
Annex D:
CHV mapping

This annex illustrates the possible CHV mappings for a single-verification capable and a multi-verification capable UICC. In the diagrams D.2 and D.3, the gray box highlights the difference between the two solutions.

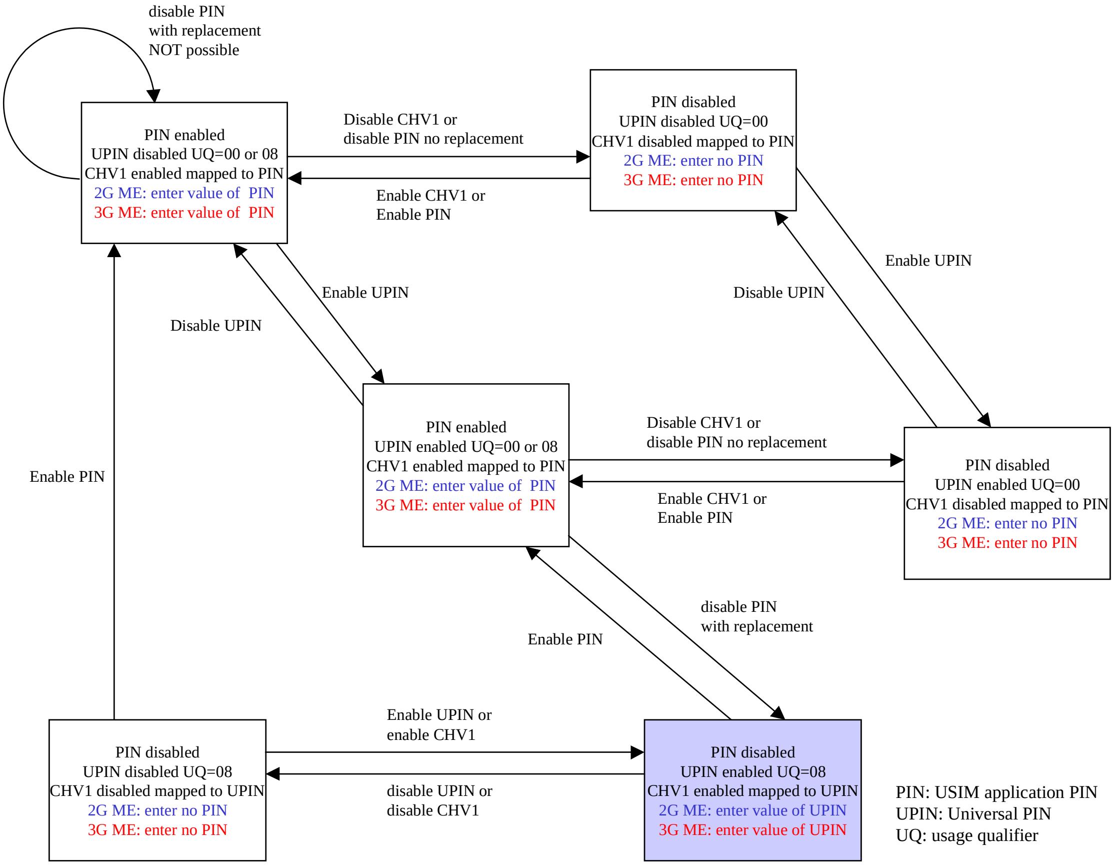
D.1 In a single-verification capable UICC


disable PIN
with replacement
NOT possible
PIN enabled
CHV1 enabled mapped to PIN
2G ME: enter value of PIN
3G ME: enter value of PIN
Disable CHV1 or
disable PIN no replacement
Enable CHV1 or
Enable PIN
PIN disabled
CHV1 disabled mapped to PIN
2G ME: enter no PIN
3G ME: enter no PIN
PIN: USIM application PIN

D.2 In a multi-verification capable UICC (static mapping)


disable PIN
with replacement
NOT possible
PIN enabled
UPIN disabled UQ=00 or 08
CHV1 enabled mapped to PIN
2G ME: enter value of PIN
3G ME: enter value of PIN
Disable CHV1 or
disable PIN no replacement
Enable CHV1 or
Enable PIN
PIN disabled
UPIN disabled UQ=00
CHV1 disabled mapped to PIN
2G ME: enter no PIN
3G ME: enter no PIN
Enable UPIN
Disable UPIN
Enable UPIN
Disable UPIN
Enable PIN
PIN enabled
UPIN enabled UQ=00 or 08
CHV1 enabled mapped to PIN
2G ME: enter value of PIN
3G ME: enter value of PIN
Disable CHV1 or
disable PIN no replacement
Enable CHV1 or
Enable PIN
PIN disabled
UPIN enabled UQ=00
CHV1 disabled mapped to PIN
2G ME: enter no PIN
3G ME: enter no PIN
disable PIN
with replacement
Enable PIN
Enable UPIN or
enable CHV1
disable UPIN or
disable CHV1
PIN disabled
UPIN disabled UQ=08
CHV1 disabled mapped to PIN
2G ME: enter no PIN
3G ME: enter no PIN
PIN disabled
UPIN enabled UQ=08
CHV1 disabled mapped to PIN
2G ME: enter no PIN
3G ME: enter value of UPIN
PIN: USIM application PIN
UPIN: Universal PIN
UQ: usage qualifier

D.3 In a multi-verification capable UICC (dynamic mapping)


disable PIN
with replacement
NOT possible
PIN enabled
UPIN disabled UQ=00 or 08
CHV1 enabled mapped to PIN
2G ME: enter value of PIN
3G ME: enter value of PIN
Disable CHV1 or
disable PIN no replacement
Enable CHV1 or
Enable PIN
PIN disabled
UPIN disabled UQ=00
CHV1 disabled mapped to PIN
2G ME: enter no PIN
3G ME: enter no PIN
Enable UPIN
Disable UPIN
Enable UPIN
Disable UPIN
Enable PIN
PIN enabled
UPIN enabled UQ=00 or 08
CHV1 enabled mapped to PIN
2G ME: enter value of PIN
3G ME: enter value of PIN
Disable CHV1 or
disable PIN no replacement
Enable CHV1 or
Enable PIN
PIN disabled
UPIN enabled UQ=00
CHV1 disabled mapped to PIN
2G ME: enter no PIN
3G ME: enter no PIN
disable PIN
with replacement
Enable PIN
Enable UPIN or
enable CHV1
disable UPIN or
disable CHV1
PIN disabled
UPIN disabled UQ=08
CHV1 disabled mapped to UPIN
2G ME: enter no PIN
3G ME: enter no PIN
PIN disabled
UPIN enabled UQ=08
CHV1 enabled mapped to UPIN
2G ME: enter value of UPIN
3G ME: enter value of UPIN

PIN: USIM application PIN
UPIN: Universal PIN
UQ: usage qualifier

Annex E: Change history

TSG # / Date	TSG Doc.	Doc 2nd level	CR	Rev	Subject/Comment	New
TP-11	TP-010045		-	-	Presented for information to TSG-T #11	1.0.0
-	-		-	-	Version after T3 AdHoc #37 (Joint with SA3), new section 4.4 inserted, section 6.1, case 5 modified	1.1.0
-	-		-	-	Version during T3#19. Minor modifications.	1.1.1
-	-		-	-	Version after T3#19 plenary presentation. Editorial modifications.	1.1.2
TP-12	TP-010113				Presented to TSG-T #12 for approval	2.0.0
TP-12	-				Approved version (includes editorial changes compared to 2.0.0)	3.0.0
TP-13	TP-010205		001	-	Sharing of enabling/disabling procedure between SIM and USIM	3.1.0
TP-15	TP-020068		002	-	Correction to SIM/USIM file mapping table	5.0.0
			004		CHV mapping, Annex D	
TP-16	TP-020119		006		Extension of Annex C - SIM/USIM file mapping table	5.1.0
			007		FDN and BDN interworking mechanism between GSM and 3G	
			008		Health warning concerning possibly different file IDs in SIM and USIM	
TP-19	TP-030030		009		Clarifying notes to SIM/USIM File Mapping Table	5.2.0
TP-21	TP-030182		010		Clarification of SIM/USIM file mapping table	5.3.0
			011		Consequences if USIM services n° 27 and n° 38 are not available.	
			012		Clarification on the interface protocol when SIM and USIM cohabit on a UICC	
TP-22	TP-030254		013		Inclusion of Rel-5 ME requirements for SIM / USIM support	5.4.0
TP-25	TP-040188		014		Correction of card operation modes	5.5.0
TP-26	TP-040266		015		Inclusion of additional USIM support for 2G terminals of R99 and Rel-4	6.0.0
TP-26	-		-		TSG-T decided to upgrade this spec to Rel-6 and withdraw Rel-5	6.0.0
TP-27	TP-050024	T3-050168	016	F	Additional USIM Support for 2G Terminals of R99 and Rel-4	6.1.0
CT-30	CP-050501	C6-050833	017	F	Mapping of EF_LOCI for SIM and USIM application	7.0.0
CT-31	CP-060025	C6-060168	022	D	Removal of 'all-release applicability' statement	7.1.0
		C6-060169	023	F	Mapping of EF-LOCIGPRS and EF-PSLOCI between SIM	
		C6-060170	024	B	Handling of ATR information for SIM and UICC	
CT-42	-	-	-	-	Upgrade to Rel-8 + addition of LTE logo	8.0.0

History

Document history		
V8.0.0	March 2009	Publication