3GPP TSG-T plenary meeting #22
Maui, US, 10-12 December 2003

Tdoc TP-030254

Source: T3

Title: CRs to TR 31.900: SIM/USIM internal and external interworking

Document for: Approval

This document contains the following change request:

Spec	CR	Rev	Phase	Subject	Cat	new ver.	Doc-2nd-Level
31.900	013	-	Rel-5	Inclusion of Rel-5 ME requirements for SIM / USIM support	F	5.4.0	T3-030939

3GPP TSG-T3 Meeting #29
Dallas, USA, 18 - 21 November 2003

Tdoc ⌘ T3-030939

CR-Form-v7

CHANGE REQUEST

⌘ **31.900** **CR** **013** ⌘ **rev** **-** ⌘ Current version: **5.3.0** ⌘

*For **HELP** on using this form, see bottom of this page or look at the pop-up text over the ⌘ symbols.*

Proposed change affects: UICC apps⌘ [X] ME [X] Radio Access Network [ ] Core Network [ ]

Title:	⌘	Inclusion of Rel-5 ME requirements for SIM / USIM support
Source:	⌘	T3
Work item code:	⌘	TEI
Date:	⌘	21/11/2003
Category:	⌘	**F**
Release:	⌘	Rel-5

Use one of the following categories:
F *(correction)*
A *(corresponds to a correction in an earlier release)*
B *(addition of feature),*
C *(functional modification of feature)*
D *(editorial modification)*
Detailed explanations of the above categories can be found in 3GPP TR 21.900.

Use one of the following releases:
2 (GSM Phase 2)
R96 (Release 1996)
R97 (Release 1997)
R98 (Release 1998)
R99 (Release 1999)
Rel-4 (Release 4)
Rel-5 (Release 5)
Rel-6 (Release 6)

Reason for change:	⌘	1. In Rel-5 some basic requirements for SIM/USIM support have changed: - For 3G MEs SIM support is now optional - For 2G MEs USIM support is now mandatory 2. Elementary File EF-RPLMNACT has been deleted from the core-specs.
Summary of change:	⌘	TR 31.900 is updated to reflect these changes
Consequences if not approved:	⌘	TR 31.900 would be inconsistent with the core-specs

Clauses affected:	⌘	Sections 3 - 6, Annex A, Annex C

Other specs affected: ⌘	Y	N		⌘
			Other core specifications	
			Test specifications	
			O&M Specifications	

Other comments: ⌘

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 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 Rel-4 or earlier, ~~It~~ 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] / TS 51.011 [8].

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, ~~two~~ 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]~~, section 10~~: "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]~~, section 11.1.3~~: "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.

For Rel-4, 3G TS 22.100 [4] does not exist. There are however similar statements in 3G TS 22.101 [5]:

- ~~In section 13:~~ "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.

- ~~In section 12.1.3:~~ "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.

Therefore, in R99 and Rel-4 we have the same situation. Note that it is not a requirement in R99 and Rel-4 that a USIM has to be supported by a 2G ME~~, with the reason that the USIM comprises new and enhanced security features which obviously cannot be supported by a 2G ME~~. Instead, in order to allow a 3G UICC to work in a 2G ME, it is feasible to put a ~~GSM~~ 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 section 13.1.3:~~ "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."

- ~~In section 14:~~ "The basic mandatory UE requirements are: Support for USIM. Optional support of GSM phase 2, 2+, 3GPP Release 99 and Release 4 SIM cards ~~[32]~~. […] 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 with Rel-5 UICCs. In this case, the Rel-4 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. ~~This is valid even when it accesses the SIM application on the UICC. According to~~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)

As ~~a~~ 2G ME of Rel-4 (or earlier) is not required to support a USIM, however this is not excluded by the standard. 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 Rel-5

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.

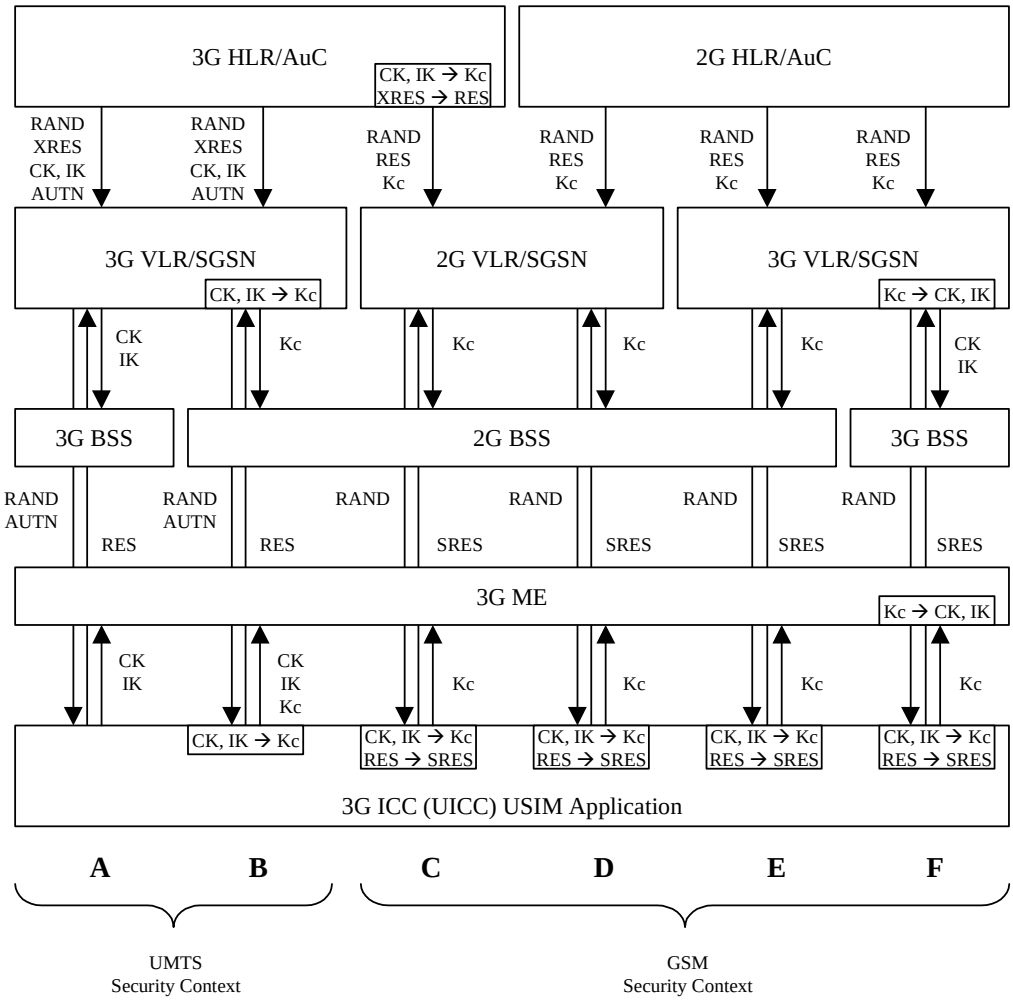

Figure 1: Possible interworking scenarios of a 3G ME and UICC with different network environments

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)

When the ME is 2G and of Rel-4 (or earlier) and 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. 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 (Rel-4 or earlier)	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.

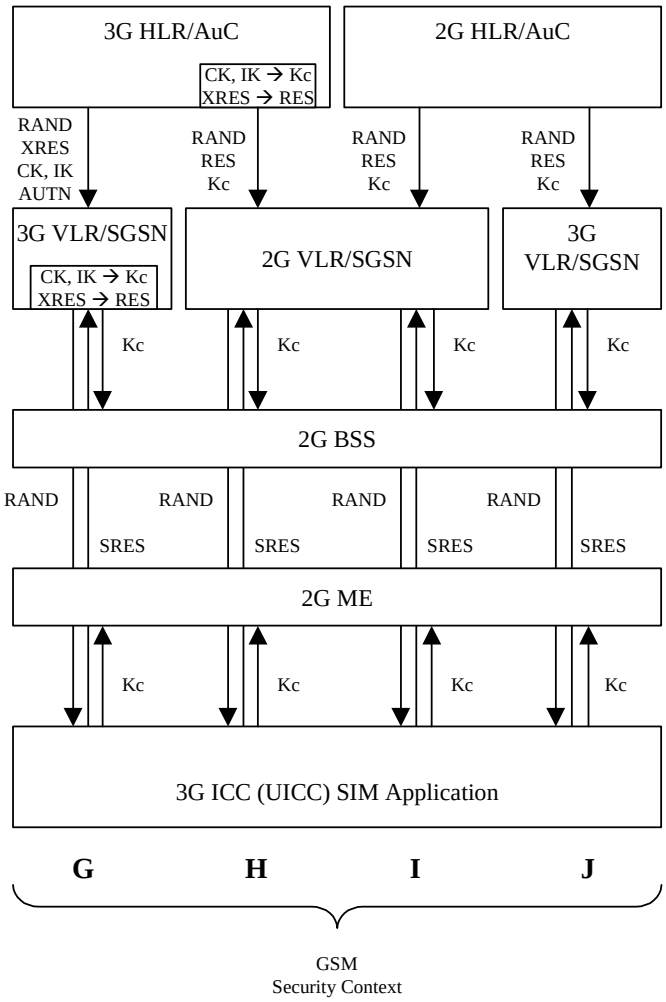

Figure 2: Possible interworking scenarios of a 2G ME and UICC with different network environments

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 Rel-5

When the ME is 2G and 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 is required to 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 (Rel-5)	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 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.

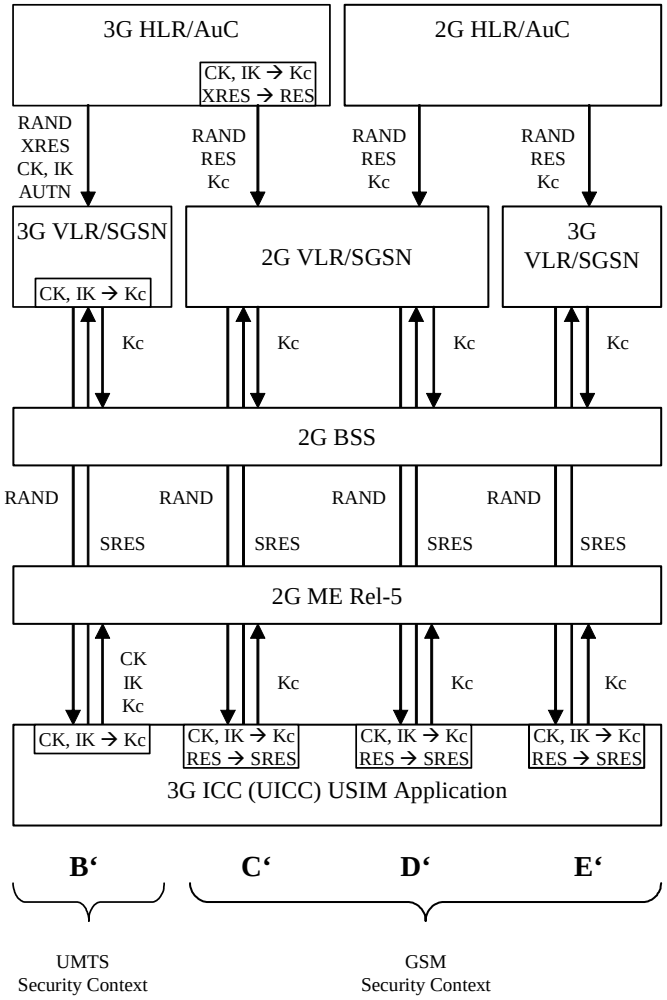

Figure 3: Possible interworking scenarios of a 2G ME and UICC with different network environments

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.

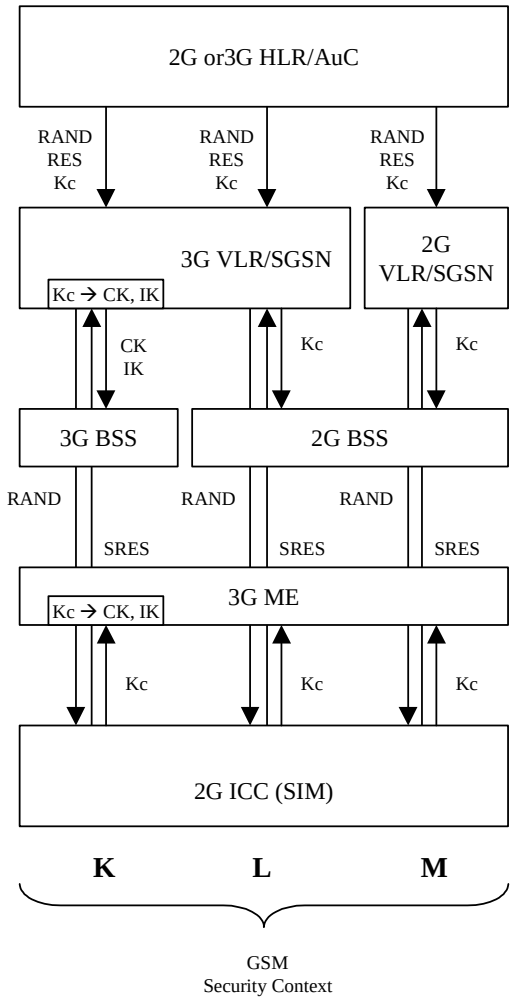

Figure ~~3~~4: Possible interworking scenarios of a 3G ME and SIM with different network environments

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 ~~and is mentioned for completeness~~. 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.

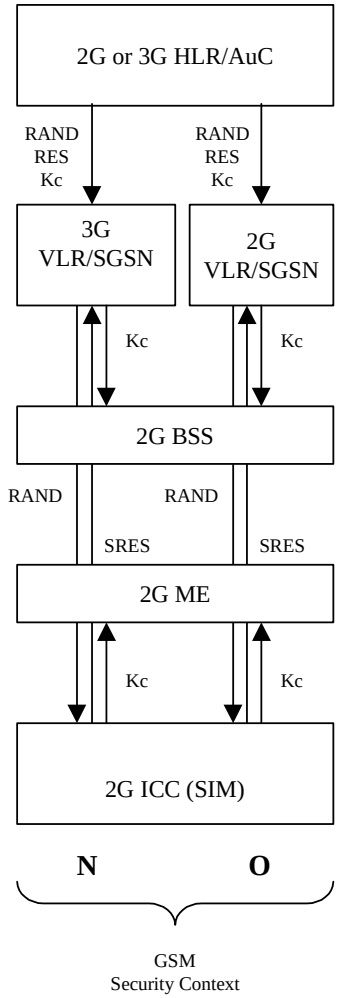

Figure 54: Possible interworking scenarios of a 2G ME and SIM with different network environments

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.

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	~~USIM incompatible with 2G ME~~						D'
3	2 7)	2	2	3	~~USIM incompatible with 2G ME~~				3G HLR/AC generates Kc from CK, IK and RES from XRES		C'
3	2 7)	2	3	2	~~USIM incompatible with 2G ME~~			3G VLR/SGSN transparent for 2G AKA			E'
3	2 7)	2	3	3	~~USIM incompatible with 2G ME~~			3G VLR/SGSN generates Kc from CK, IK			B'
3	2	3	2	2	~~USIM incompatible with 2G ME~~		3G BSS incompatible with 2G ME				
3	2	3	2	3	~~USIM incompatible with 2G ME~~		3G BSS incompatible with 2G ME				
3	2	3	3	2	~~USIM incompatible with 2G ME~~		3G BSS incompatible with 2G ME				
3	2	3	3	3	~~USIM incompatible with 2G ME~~		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
2) 2G/3G dual mode ME required, no service otherwise
3) Support of service n° 27 required in the USIM, no service otherwise
4) Support of services n° 27 and n° 38 required in the USIM, no service otherwise
5) 2G ME of Rel-4 (or earlier) or of Rel-5 with (optional) SIM support
6) 3G ME of Rel-4 (or earlier) or of Rel-5 with (optional) SIM support
7) 2G ME of Rel-5. No service with 2G ME of Rel-4 or earlier
8) 2G ME of Rel-4 (or earlier)

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	
GSM / LOCIGPRS	USIM / PSLOCI	yes, 5)	
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 / RPLMNACT~~	~~USIM / RPLMNACT~~	~~no~~	
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
2) SIM file to be mapped with related USIM file either in DF PHONEBOOK under DF USIM or in DF PHONEBOOK under DF TELECOM
3) Only if the same settings apply to 2G and 3G operation
4) No mapping of EF-MSISDN if EF-EXT1 is used in the SIM and / or EF-EXT5 is used in the USIM
5) Caution: Different file identifiers in SIM and USIM
6) No mapping if coding "FF" is used in the content
7) Mapping is possible only if the size of FPLMN is 12 bytes.