3GPP TSG SA WG3 Security — S3#16 **S3-000661**

3GPP T3 Meeting #16 ***Tdoc T3-000509***

Seoul, Korea, 13 - 15 November, 2000

3G TR ab.cde V0.0.1 (2000-11)

Technical Report

3rd Generation Partnership Project; Technical Specification Group Terminals; SIM/USIM Internal and External Interworking Aspects (Release 1999)

Keywords

SIM, USIM, UICC

3GPP

Postal address

3GPP support office address

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

Internet

http://www.3gpp.org

Contents

Foreword

This Technical Report (TR) 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 UMTS-UICC) and a GSM or UMTS 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 shall give a guideline 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] 3G TS 31.101: "UICC-Terminal Interface; Physical and Logical Characteristics"

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

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

[4] 3G TS 22.100: "UMTS Phase 1"

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

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

[6] GSM TS 11.11: "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 Center
BSS	Base Station Subsystem
CK	Cipher Key
GSM	Global System for Mobile Communication
HLR	Home Location Register
ICC	Integrated Circuit Card
IK	Integrity Key
ME	Mobile Equipment
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
XRES	Authentication value delivered by the 3G HLR/AuC
UICC	UMTS Integrated Circuit Card
UMTS	Universal Mobile Telecommunication System
USIM	UMTS Subscriber Identity Module
VLR	Visitor Location Register

4 Primary clarifications and definitions

For the purpose of this report the following clauses shall 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.

The abbreviation 3G stands for 3rd generation technology and characterises elements of a mobile communication system which are based on the UMTS standard, i.e. 3G 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 UMTS 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 (or GSM and UMTS) only, with the relationship given by

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

3G = UMTS = UMTS 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.

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.

The UICC is the physical and logical platform for the USIM. It shall 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.

4.3 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 GSM. In a mixed 2G/3G network environment 2G AKA is performed when - except for the BSS - at least one other network 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. For 3G AKA all involved network 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

UMTS is designed to be compatible with GSM and several interworking requirements apply. Regarding the ICC/ME interface, two basic requirements can be identified in the 3G standards:

- In 3G TS 22.100, 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 3G ME shall support a 2G ICC.
- In 3G TS 22.101, 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 UICC may contain a SIM application.

Note that it is not a requirement that a USIM shall be supported by a 2G terminal, 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 application (according to GSM TS 11.11) onto the UICC in addition to the USIM.

For the ICC/ME interface, with two main types of ME and two main types of ICC, four different scenarios can be identified. They are described in the following sections.

5.1 3G ME and UICC

A 3G or 2G/3G dual mode ME shall support the UICC. After it has activated the UICC, it shall immediately select a USIM application. 3G TS 31.101 and 3G TS 31.102 apply.

According to 3G TS 21.111 a 3G terminal shall not support a 5V ME/UICC interface. This is valid even when it accesses the SIM application on the UICC. According to the same specification, a UICC shall 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, only the USIM application can be activated by the ME, i.e. nothing but the 3G command set (as defined in 3G TS 31.101 and 3G TS 31.102) 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. 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.
2. **Service n° 38:** "GSM Security Context". This service is required when a 2G VLR 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).

   A 2G VLR never goes with a 3G BSS. Hence when a 2G VLR is involved, then a 2G BSS is always part of the transmission chain. This means that service n° 27 is additionally required, i.e. services n° 27 and n° 38 have to be available at the same time (when a 2G VLR is involved). There is only one possible situation, in which service n° 38 makes sense on its own: If a USIM subscription is kept in a 2G HLR/AuC and - with a 3G ME - roams in a 3G network, see also section 6.1, case 5.

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 shall always access 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.

5.2 2G ME and UICC

As a 2G ME is not required to support a USIM, this combination will only work if a SIM application is provided by the UICC. GSM 11.11 applies.

5.3 3G ME and SIM

A 3G or 2G/3G dual mode ME shall support a SIM - even if it is not residing on a UICC. For this purpose it has to provide a SIM interface in addition to the 3G UICC interface. Access is possible to both 3G and 2G networks. GSM 11.11 applies.

According to 3G TS 21.111 a 3G terminal shall not support a 5V ME/UICC interface. This does not exclude that the terminal supports a 5V ME/SIM interface to be compatible with (old - but still existing) 5V only SIMs.

5.4 2G ME and SIM

This is the well-known 2G case. GSM 11.11 applies. Access to 3G networks is not possible with this combination.

6 Authentication and key agreement in mixed networks

The authentication and key agreement procedure basically involves five network components (ICC, ME, BSS, VLR and HLR/AuC), 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. 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	HLR/AuC	Service	Figure 1
1	3G	3G	3G	3G	3G	yes	A
2			2G	3G	3G	yes 1) 4)	B
3			3G	2G	3G	no	
4			2G	2G	3G	yes 3) 4)	C
5			3G	3G	2G	yes 2)	F
6			2G	3G	2G	yes 3) 4)	E
7			3G	2G	2G	no	
8			2G	2G	2G	yes 3) 4)	D

Note: 1) requires service n° 27 supported by the USIM
2) requires service n° 38 supported by the USIM
3) requires services n° 27 and n° 38 supported by the USIM
4) 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 (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 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 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 which is 2G. As a 2G VLR 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 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 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. Between the VLR 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.

Case 5: All system elements are 3G, except for the HLR/AuC, which is 2G. It is possible to keep a USIM subscription in a 2G HLR/AuC AuC, however on request by a 3G VLR this can only deliver 2G triplets RAND, RES and Kc. Since the 3G BSS requires ciphering and integrity protection keys CK and IK, these have to be generated by the 3G VLR, which therefore applies conversion functions c4 and c5. The 2G authentication parameter RAND however is transmitted transparently through the 3G BSS and the ME to the USIM. 2G AKA is executed. Just like the VLR the ME has to convert the received Kc into CK and IK by also using conversion functions c4 and c5. SRES is transmitted back to the VLR.

If the USIM does not support service n° 38, network access is not possible. As a 2G BSS is not involved, support of service n° 27 is not necessary in this case.

This scenario is marked with "F" in figure 1.

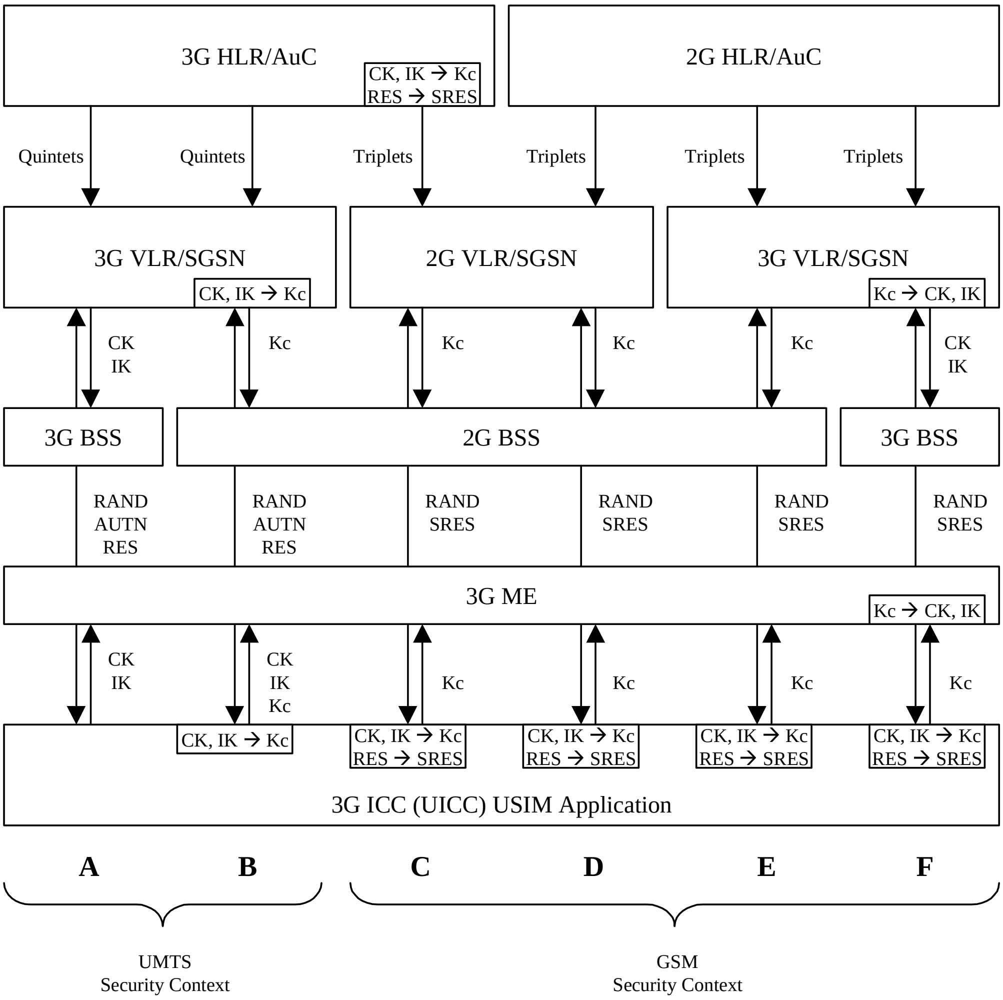

Figure 1: Possible interworking scenarios of a 3G ME and UICC with different network environments

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 this can only deliver 2G triplets RAND, RES and Kc. The 3G VLR is backward compatible and behaves like a 2G VLR: Between the VLR 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 and the HLR/AuC, which are 2G. The situation is the same as in case 3 above: As a 2G VLR 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 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

When the ME is 2G 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	HLR/AuC	Service	Figure 2
1	3G with SIM Appl.	2G	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. 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 (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 is already 3G).

Upon request from a 3G VLR, the 3G HLR/AuC delivers quintets. The VLR, since a 2G ME is involved, performs 2G AKA, i.e. it generates Kc from CK, IK (conversion function c3) and forwards RAND to the BSS. The rest is straight forward and follows the 2G procedure. In the UICC only the SIM application is active.

This scenario is marked with "G" in figure 2.

Case 4: ME, BSS and VLR 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, 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. 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.

Case 6: ME, BSS and HLR/AuC are 2G, ICC and VLR 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 and 2G BSS technology.

Since the 3G VLR 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 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.

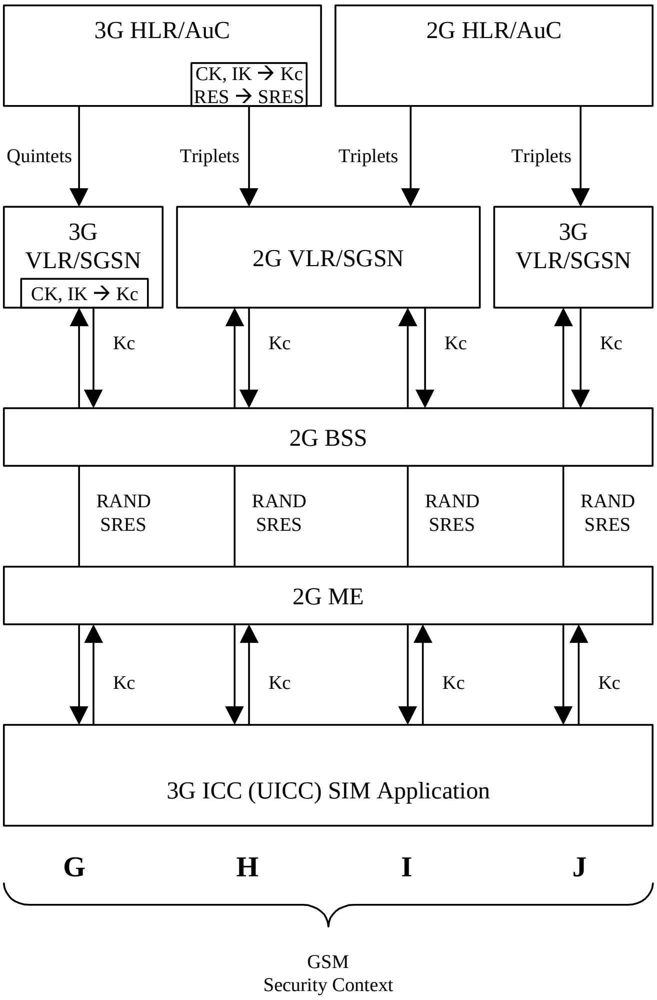

Figure 2: Possible interworking scenarios of a 2G ME and UICC with different network environments

6.3 With 3G ME and SIM

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	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 are 3G, the ICC is 2G (i.e. a SIM) and the HLR/AuC is "don't care". 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. The 3G BSS requires CK and IK, so the VLR 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, IK, security is based on Kc, i.e. 2G security context is established.

This scenario is marked with "K" in figure 3.

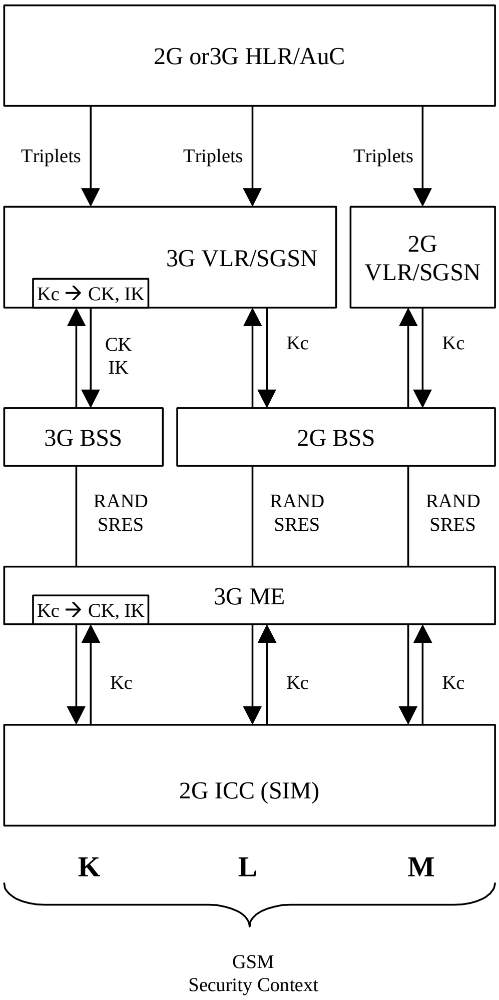

Figure 3: Possible interworking scenarios of a 3G ME and SIM with different network environments

Case 2: ME and VLR are 3G, ICC and BSS are 2G and the HLR/AuC is "don't care". 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 and in the ME. Both, the 3G VLR 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 are 2G and the HLR/AuC is "don't care". As a 2G VLR and a 3G BSS are not compatible, this theoretical combination cannot exist. No service in this case.

Case 4: ICC, BSS and VLR are 2G, the ME is 3G and the HLR/AuC is "don't care". 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.

6.4 With 2G ME and SIM

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	HLR/AuC	Service	Figure 4
1	2G	2G	3G	3G	2G or 3G	yes	
2			2G	3G		yes	N
3			3G	2G		no	
4			2G	2G		yes	O

Cases 1, 3: A 3G BSS does not work in combination with a 2G VLR. No service in these cases.

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

This scenario is marked with "N" in figure 4.

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.

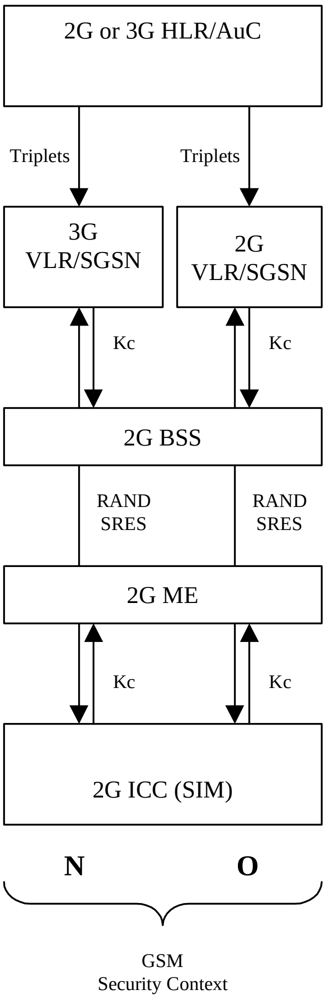

Figure 4: Possible interworking scenarios of a 2G ME and SIM with different network environments

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

TBD

8 Interworking between USIM applications on a UICC

TBD

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 figures 1 to 4 in section 6.

ICC	ME	BSS	VLR	AUC	ICC	ME	BSS	VLR	HLR/AuC	Security Context	
2	2	2	2	2						2G	O
2	2	2	2	3					3G HLR/AC generates 2G triplets for 2G IMSI	2G	O
2	2	2	3	2				3G VLR transparent for 2G AKA		2G	N
2	2	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				
2	2	3	2	3			3G BSS incompatible with 2G ME and 2G VLR				
2	2	3	3	2			3G BSS incompatible with 2G ME				
2	2	3	3	3			3G BSS incompatible with 2G ME				
2	3	2	2	2		3G ME transparent for 2G AKA 2)				2G	M
2	3	2	2	3		3G ME transparent for 2G AKA 2)			3G HLR/AC generates 2G triplets for 2G IMSI	2G	M

2	3	2	3	2		3G ME transparent for 2G AKA 2)		3G VLR transparent for 2G AKA		2G	L
2	3	2	3	3		3G ME transparent for 2G AKA 2)		3G VLR 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				
2	3	3	2	3			3G BSS incompatible with 2G VLR				
2	3	3	3	2		3G ME transparent for 2G AKA, generates CK, IK from Kc	3G BSS transparent for 2G AKA	3G VLR transparent for 2G AKA, generates CK, IK from Kc		2G	K
2	3	3	3	3		3G ME transparent for 2G AKA, generates CK, IK from Kc	3G BSS transparent for 2G AKA	3G VLR transparent for 2G AKA, generates CK, IK from Kc	3G HLR/AC generates 2G triplets for 2G IMSI	2G	K
3	2	2	2	2	USIM incompatible with 2G ME						
3	2	2	2	3	USIM incompatible with 2G ME						
3	2	2	3	2	USIM incompatible with 2G ME						
3	2	2	3	3	USIM incompatible with 2G ME						
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						
3	2	3	3	3	USIM incompatible with 2G ME						
3	3	2	2	2	2G mode 5)	3G ME transparent for 2G AKA 2)				2G	D
3	3	2	2	3	2G mode 5)	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 5)	3G ME transparent for 2G AKA 2)		3G VLR transparent for 2G AKA		2G	E
3	3	2	3	3	3G + Kc mode 3)	2)		3G VLR generates Kc from CK, IK		3G	B
3	3	3	2	2			3G BSS incompatible with 2G VLR				
3	3	3	2	3			3G BSS incompatible with 2G VLR				
3	3	3	3	2	2G mode 4)	3G ME transparent for 2G AKA, generates CK, IK from Kc		3G VLR transparent for 2G AKA, generates CK, IK from Kc		2G	F
3	3	3	3	3						3G	A
3 1)	2	2	2	2	SIM appl. active					2G	I
3 1)	2	2	2	3	SIM appl. active				3G HLR/AC generates Kc from CK, IK and RES from XRES	2G	H
3 1)	2	2	3	2	SIM appl. active			3G VLR transparent for 2G AKA		2G	J
3 1)	2	2	3	3	SIM appl. active			3G VLR transparent for 2G AKA, generates CK, IK from Kc		2G	G
3 1)	2	3	2	2			3G BSS incompatible with 2G ME and 2G VLR				
3 1)	2	3	2	3			3G BSS incompatible with 2G ME and 2G VLR				
3 1)	2	3	3	2			3G BSS incompatible with 2G ME				
3 1)	2	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 service n° 38 required in the USIM, no service otherwise
5) Support of services n° 27 and n° 38 required in the USIM, no service otherwise

Annex B: Features for security interworking

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

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 (done in the AuC or the VLR) or a 3G authentication response RES into a 2G authentication response SRES (done 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 $(X)RES_{3G} = (X)RES_{3G,\,1}$ [|| xor $(X)RES_{3G,\,2}$ [|| xor $(X)RES_{3G,\,3}$ [|| xor $(X)RES_{3G,\,4}$]]] depending on the length of (X)RES (a multiple of 32 bit). 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° 27 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 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° 38 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.

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.

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 and 3G TS 33.102.

In **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: Change history

Change history							
Date	**TSG #**	**TSG Doc.**	**CR**	**Rev**	**Subject/Comment**	**Old**	**New**
2000-11	-	-	-	-	First draft version created by rapporteur for discussion at T3 #16 as part of the work for the T3 work item "Report on SIM.USIM interworking"		0.0.1