3GPP TSG SA WG3 Security — S3#20 **S3-010468**

16 - 19 October, 2001

Sydney, Australia

Source: **Telia**

Title: **ISIM/USIM independence**

Document for: **Information**

Agenda Item: **IMS Security**

Security considerations for IMS access independence

Contents **Page**

1 Introduction 2

2 Definitions 2

3 Access independence to IP Multimedia Subsystem 2
3.1 Introduction 2
3.2 USIM/ISIM independence 3
3.3 USIM/ISIM split considerations 5
3.3.1 ISIM and USIM on separate ICCs 5
3.3.2 ISIM and USIM on same ICC 6
3.3.3 UE split consideration 7

4 Terminal issues 7
4.1.1 IETF SIP vs IMS SIP clients 7
4.1.2 Card reader issues 7

5 Access to the ISIM application and the USIM application 8

6 Network Domain Security and access independence 9

7 Conclusions 10

8 References 11

Introduction

Since there exist no clear definition in any 3GPP specification (not within the writers knowledge) of what access independence really means, this document has been based on Telias interpretation of the concept.

In [4], it is stated that the IMS shall be access independent. Telia's understanding of "access independence" is that IMS should be accessible from a variety of IP based access technologies. This PM is for information and its intention is to bring up some issues that are inconsistent with the statement in [4]. In addition, the work on splitting the UE is not possible, with the current coupled definitions of USIM, ISIM and UICC.

Definitions

The following definitions are presently stated in TS 21.133 (3G Security; Security Threats and Requirements)[1], TS 33.203 (Access security for IP-based services)[2] and TR 21.905 (Vocabulary for 3GPP Specifications) [3].

"UMTS Integrated Circuit Card (UICC): a physically secure device that can be inserted and removed from terminal equipment. It can contain one or more applications one of which must be the USIM"[1]

"UMTS IC Card: An IC card (or 'smartcard') of defined electromechanical specification which contains at least one USIM" [3]

"User Services Identity Module (USIM): an application that represents and identifies a user and his association with a home environment in the provision of 3G services. The USIM contains functions and data needed to identify and authenticate users when 3G services are accessed. It may also contain a copy of the user's service profile. It may also provide other security features. The USIM contains the user's IMUI and any security parameters, which need to be carried by the user. The USIM is always implemented in a removable IC card called the UICC." [1]

"Universal Subscriber Identity Module (USIM): An application residing on the UICC used for accessing services provided by mobile networks, which the application is able to register on with the appropriate security." [3]

"ISIM – IM Services Identity Module. In a security context, this module is responsible for performing subscriber and network authentication and key agreement in IM CN SS. The ISIM resides on the UICC." [2]

From these definitions, we conclude that the ISIM and the USIM must reside on the same physical UICC.

Access independence to IP Multimedia Subsystem

Introduction

In [4], it is stated that the IMS shall be access independent. Telia's understanding of "access independence" is that IMS should be accessible from a variety of IP based access technologies, e.g. UMTS, WLAN and ADSL (see Figure 1). Further, the IMS subscriber should be able to use the same procedures when registering or setting up sessions independently of access technology.

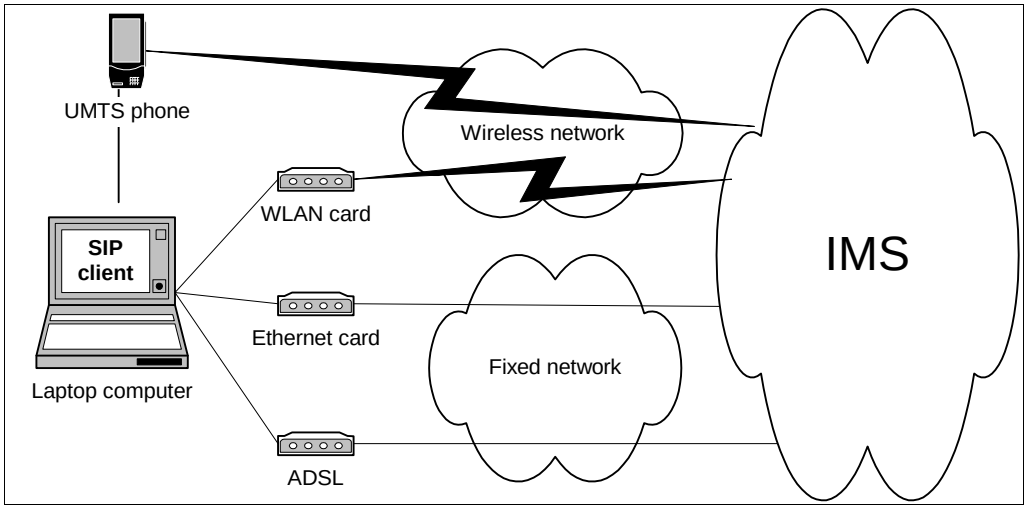

Figure 1 IMS access independence

Another aspect is terminal independence. From an IMS user perspective, it should be as easy accessing IMS services from a laptop or desktop computer as accessing IMS services from a UMTS terminal.

As stated in [2], the security functionality of IMS should be independent of UMTS security. It is also an important issue to achieve access independence.

In order to fulfil complete access independence, some issues have been identified. These are presented in the following sections.

USIM/ISIM independence

It is stated in [2] that IMS security functionality should be independent from UMTS security. The UE split discussion in Newbury identified problems with the current architecture [5]. In order to fulfil this requirement when we have a split UE, the ISIM must be separated from the USIM, not only logical, as in the current standard [2], but also physical separation is necessary. To get access independence a user should not be forced to have a UMTS subscription, an IMS subscription should be enough.

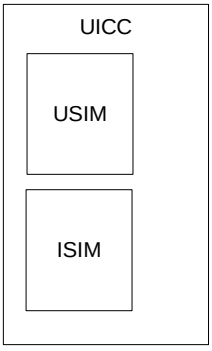

Figure 2 UICC with ISIM (and USIM)

According to the definition of ISIM, USIM and UICC (see definitions above) this is not possible. The UICC must include a USIM and the ISIM must reside on the UICC. This implies that in order to have an IMS subscription (ISIM) a user must have a UMTS subscription (USIM) and both SIMs must reside on the UICC.

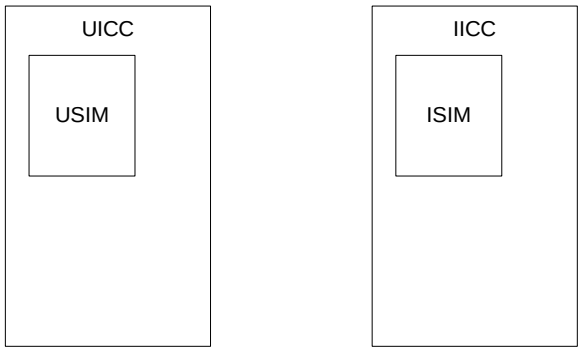

Figure 3 USIM and ISIM independence

The ISIM need the same physical security as the USIM, i.e. the ISIM must reside on a tamper proof ICC (Integrated Circuit Card) like the USIM. One idea would be to define a IMS Integrated Circuit Card (IICC) that contains the ISIM. This would be used in cases when it is not desired to have the ISIM on the UICC, for example when UMTS is not used for access to IMS. This IICC could be a physical card similar to the UICC, with the intention to contain the ISIM not the USIM.

The definition of ISIM also needs to be redefined to state that the ISIM is independent of the UICC.

Below suggestions for definitions are presented:

New definition:

"IMS Integrated Circuit Card (IICC): a physically secure device that can be inserted and removed from terminal equipment. It can contain one or more applications one of which must be the ISIM"

Change of definition:

"ISIM – IM Services Identity Module. In a security context, this module is responsible for performing subscriber and network authentication and key agreement in IM CN SS. The ISIM resides on the UICC or the IICC."

USIM/ISIM split considerations

This section brings up some problems related to storing the ISIM and the USIM on separate UICC and IICC vs. storing them on the same ICC (UICC).

ISIM and USIM on separate ICCs

The figure below shows the main advantages using separate ICCs. A user can easily move from one access technology to another and still use IMS. The user is not bound to a UMTS subscription and no sensitive information, such as keys, needs to be transferred between the separate IMS client (on a PC) and the UMTS terminal.

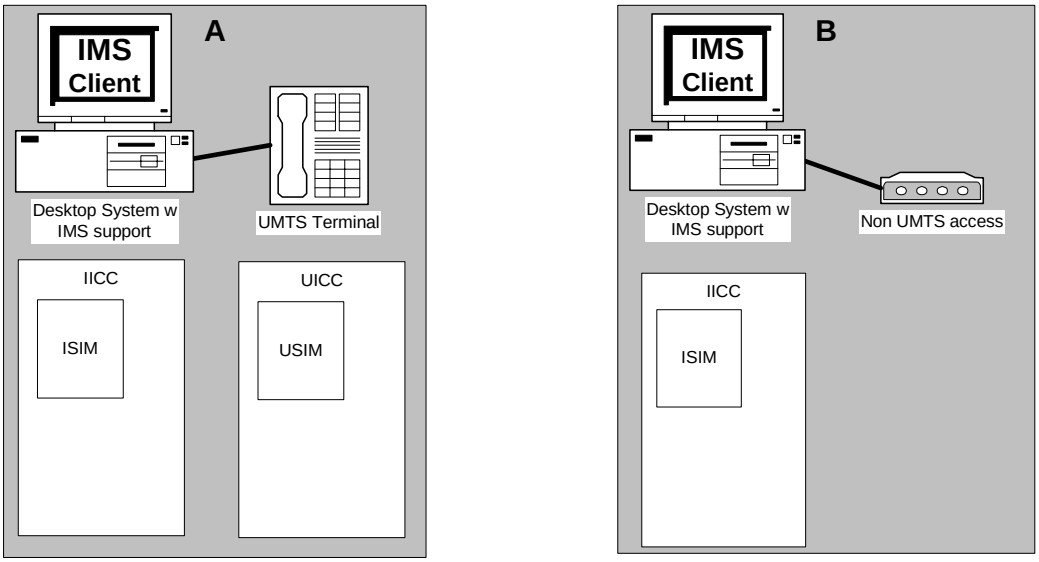

Figure 4 Separate ISIM and USIM ICC

A drawback with using separate ICCs is that access to the IMS through UMTS requires two card readers, one card reader for the actual IMS access and one for the UMTS access. If the IMS client is separated from the UMTS terminal (see figure above), any IMS client terminal (e.g. a PC) need to be equipped with a card reader.

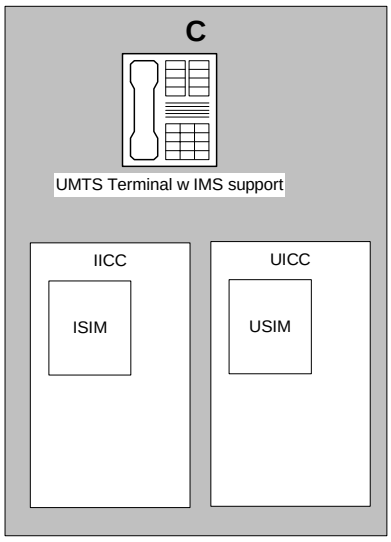

Figure 5 Separate ISIM and USIM ICC (access to IMS through UMTS using combined IMS/UMTS terminal)

If the IMS client is integrated into the UMTS terminal, it is required that the terminal has two card readers (see figure above).

ISIM and USIM on same ICC

In the case when the ISIM and USIM are located on the same ICC (UICC), the following issues need to be considered.

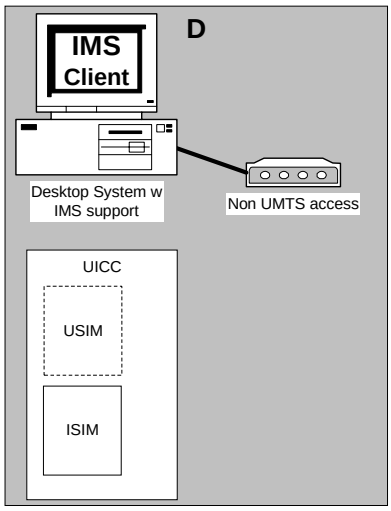

Figure 6 Access to IMS through non-UMTS (no UMTS terminal)

When accessing IMS using a non-UMTS access, the IMS client should only have access to the ISIM and not the USIM, i.e. the USIM should be inactive (see figure above).

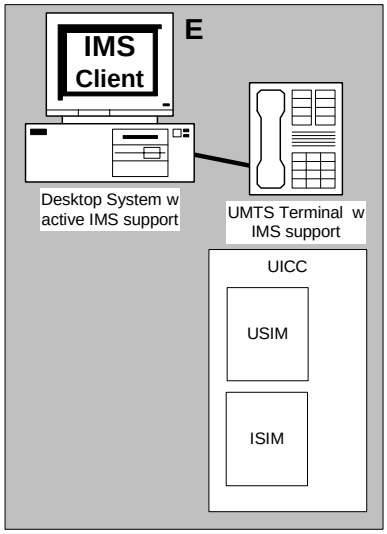

Figure 7 Access to IMS through UMTS (separate IMS and UMTS terminal)

The use of an ICC, which contains both the USIM and the ISIM (see figure above) makes access to IMS through a separate IMS client (for example on a PC) impossible. The IMS client on the PC need to access the ISIM which is located on the UICC (the UICC is in the UMTS terminal) through some interface between the PC and UMTS terminal. (UE split ?)

This could possibly be solved by using two ICCs (see figure below). One ICC (UICC) that contains the USIM and ISIM for use when the IMS client and UMTS terminal are integrated, and one ICC (IICC) to use when a separate IMS client (a PC) is used.

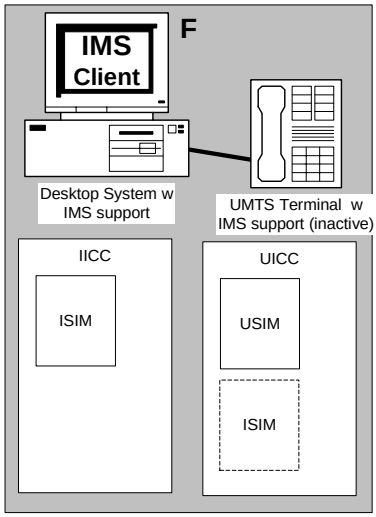

Figure 8

In such a solution, it is important that there exists some mechanism that makes the ISIM on the UICC inactive in order to use the ISIM on the IICC (the separate IMS client, e.g. a PC).

Note, the long-term key stored on the ISIM and in the HSS is associated to the IM Private Identity (IMPI) [2], and a subscription can only have one IMPI [9]. Does this not make two ISIMs impossible for one subscription? (This solution needs further study)

UE split consideration

The use of a separate ISIM on a IICC removes the problem of transferring sensitive security information over any UE – TE interface.

Terminal issues

IETF SIP vs IMS SIP clients

As stated above, from an IMS user perspective, it should be as easy accessing IMS services from a laptop or desktop computer as accessing IMS services from a UMTS terminal. Since future operating systems are expected to have pre-installed standard (IETF) SIP clients, it is important that the IMS SIP and the IETF SIP clients are identical according to standards. If this is not done, a non-UMTS user with an ordinary “IETF SIP client” might not be able to access IMS because of compatibility problems between the SIP client and the IMS. One such example is the IMS AKA extension, if it is not included in the IETF SIP, there will be compatibility problems!

Card reader issues

Every terminal used for accessing the IMS needs to have a card reader for the ICC and this might be non- user friendly. One of the basic ideas with SIP is user mobility; a user should be able to register at the SIP server independently of terminal. The use of an ICC makes this difficult. From a security point of view it is of course necessary to use an ICC, but it will make the use of IMS services limited to those terminals with proper card readers.

Another aspect is the card reader interface. Any IMS SIP client needs a driver for the card reader. If the interface between the card reader and the operating system does not follow a widely deployed standard a special driver is needed and this might also be a problem (need further study).

Access to the ISIM application and the USIM application

In order to separate the different applications on the ICC (in case the USIM and the ISIM are located on the same ICC) it might be necessary to use different PIN codes for the ISIM application and the USIM application. This means that a "Universal PIN" as defined in [8] should not be allowed. If allowed, it is possible for a client application to access both applications on the ICC using the same PIN, and this might not be good from a security point of view.

Consider the following scenario:

A user with a UICC containing the ISIM and the USIM (the same PIN is used for accessing both the ISIM and the USIM) enters an Internet cafe and uses the provided PC with an installed IMS client to access IMS. The user accesses IMS through the Internet, not UMTS (see figure below). The user enters his/her PIN code (on the PC) to make it possible for the IMS client on the PC to connect to the selected IMS. The installed IMS client is "malicious" and starts accessing information stored on the USIM. The goals for such attacks could be to gather enough information from the USIM in order to clone it, or perform active cryptographic attacks. If different PIN codes where used, the malicious client on the PC would only have access to the ISIM. The threat still exists for the ISIM though, but the damage is only limited to the ISIM.

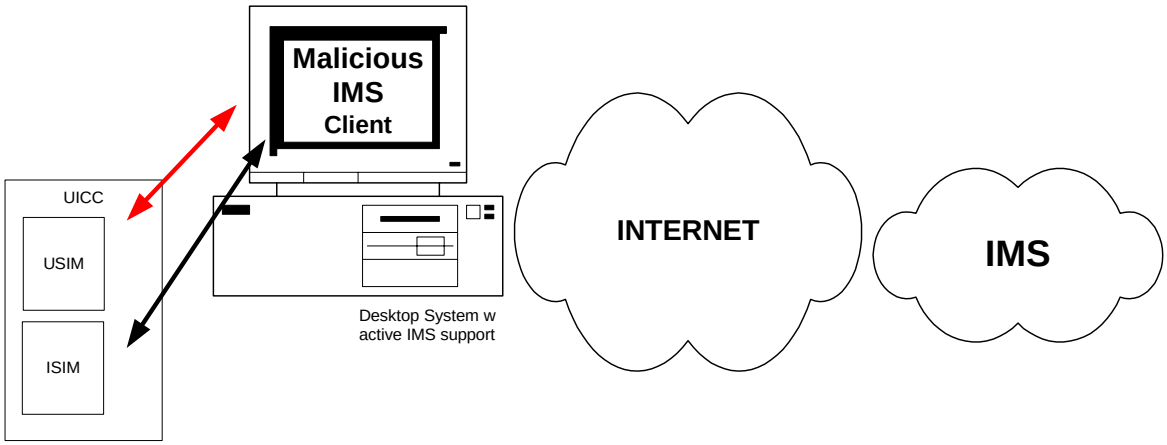

Figure 9 Malicious IMS client

The use of two separate PIN codes for the USIM/ISIM might be bad from a user perspective when using an IMS client integrated with a UMTS terminal, since the user need to enter two PINS. This could be solved by using one PIN that opens up both the USIM and the ISIM, and this would be used in the case when the IMS client is integrated with the UMTS terminal. Another PIN only opens up the ISIM and would be used in the separate IMS client case (i.e. IMS client on a PC)

The USIM seems tightly connected to the "closed" UMTS world, the software used in the UMTS terminals are within the control of the manufactures and operators. The ISIM on the other hand has not this tight coupling since IMS is supposed to be access independent. It is possible for "uncontrolled applications" in a PC to access the UICC. This is a reason for why different PIN codes might be a thing to consider.

"A multi-application capability UICC (from the security context point of view) shall support the replacement of a USIM application PIN with the Universal PIN, key reference '01', as defined in 3G TS 31.101 [11]. Only the Universal PIN is allowed as a replacement"[7]

This means that a user can change the use of application PINs to the use of one Universal PIN for accessing both the USIM and the ISIM, unless the technical specifications [7][8] are altered. Assumably this issue has already been considered and it has been decided that it should NOT be possible to require only application PINs on a multi-application UICC (i.e. not possible to forbid the use of a Universal PIN).

Network Domain Security and access independence

According to the IMS security specification [2] there exists a security association (SA) between the P-SCSF and the I-CSCF (or S-CSCF). This SA (4) is depicted in the figure below. How this should be handled is not covered in [2], instead the NDS/IP specification [6] specifies what security measures shall be defined for these types of interfaces.

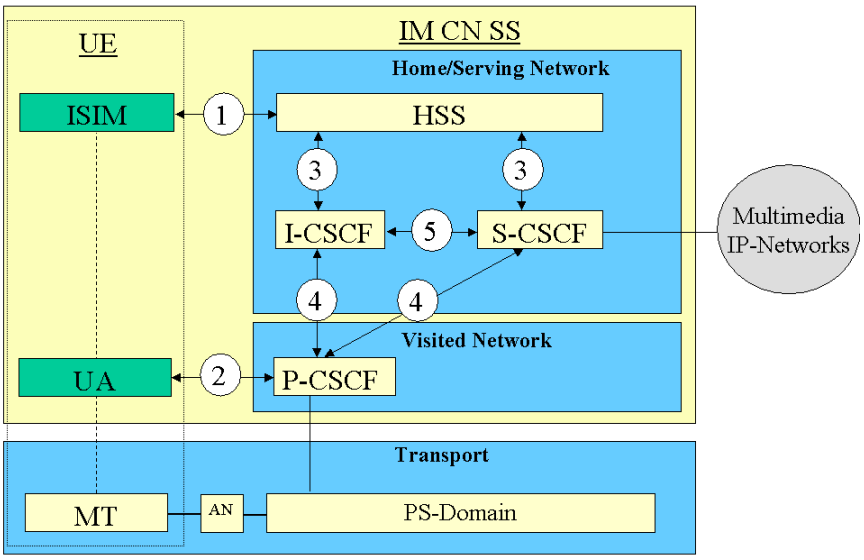

Figure 10 IMS security

In [6] it is stated that all traffic shall pass through a security gateway (SEG) before entering or leaving a security domain, this implies that SEGs must exist between the P-CSCF and the I-CSCF (or S-CSCF), as depicted in the figure below.

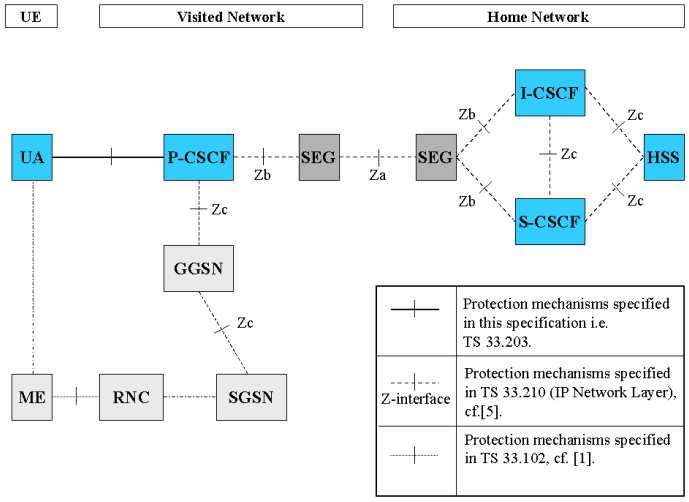

Figure 11 NDS/IP and IMS security

To set-up the required IPSec tunnel between two SEGs, IPSec SAs are needed. These SAs are established under the protection of a IKE SA. In order to establish the IKE SA, the SEGs need to be mutually authenticated and this is carried out during the first phase of IKE.

This affects the access independence, since any visited network need to be able to establish a IPSec tunnel between the SEG (P-CSCF) in the visited network and the SEG (I-CSCF/S-CSCF) in the home network. Since IKE is supposed to be used for key management, the SEG in the visited network need to share IKE authentication keys with the SEG in the home network or a Key Distribution Center (KDC). If a user arrives in a visited network that does not support this, access to IMS is not possible.

Conclusions

From the short analysis presented in this document it is clear that the access independence requirement for IMS stated in [4] introduces some problems for the IMS security architecture. In order to adapt the IMS security architecture towards access independence some modifications are needed. The separation of the USIM and the ISIM has been the main focus of this document but other issues, such as the close connection to NDS, have also been identified. There will probably come up other issues related to access independence and IMS security as the work continues. Most of the issues brought up in this document are based on Telias interpretation of the concept “access independence”. To get a deeper understanding of the concept access independence a clear definition is needed from 3GPP.

References

[1] 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3G Security; Security Threats and Requirements (3G TS 21.133 version 3.1.0)

[2] 3rd Generation Partnership Project; Technical Specification Group SA3; Access security for IP-based services (Release 5) 3G TS 33.203 V0.5.0 (2001-06)

[3] Universal Mobile Telecommunications System (UMTS);Vocabulary for 3GPP Specifications (3GPP TR 21.905 version 4.3.0 Release 4) (2001-06)

[4] 3rd Generation Partnership Project;Technical Specification Group Services and System Aspects; Service requirements for the IP Multimedia Core Network Subsystem (Stage 1) (Release 5) 3GPP TS 22.228 V5.2.0 (2001-06)

[5] Draft report for joint S1/S3/T2/T3 meeting about security implications of UE functional split 3rd July 2001 - version 0.0.3

[6] 3G TS 33.210: "3rd Generation Partnership Project (3GPP); Technical Specification Group (TSG) SA; 3G Security; Network domain security; IP network layer security".

[7] Universal Mobile Telecommunications System (UMTS); Characteristics of the USIM Application 3GPP TS 31.102 version 4.1.0 (Release 4)

[8] Smart cards;UICC-Terminal interface; Physical and logical characteristics (Release 4) ETSI TS 102 221 V4.2.0 (2001-04)

[9] 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; IP Multimedia (IM) Subsystem - Stage 2 (Release 5) 3GPP TS 23.228 V5.1.0 (2001-06)