3GPP TSG SA WG3 Security — IMS Security ad-hoc **S3z010100**

14 September, 2001

Sophia Antipolis, France

Source: **Telia**

Title: **ISIM/USIM independence**

Document for: **Information**

Agenda Item: **8 (AOB)**

IMS Access independent issues

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. 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.

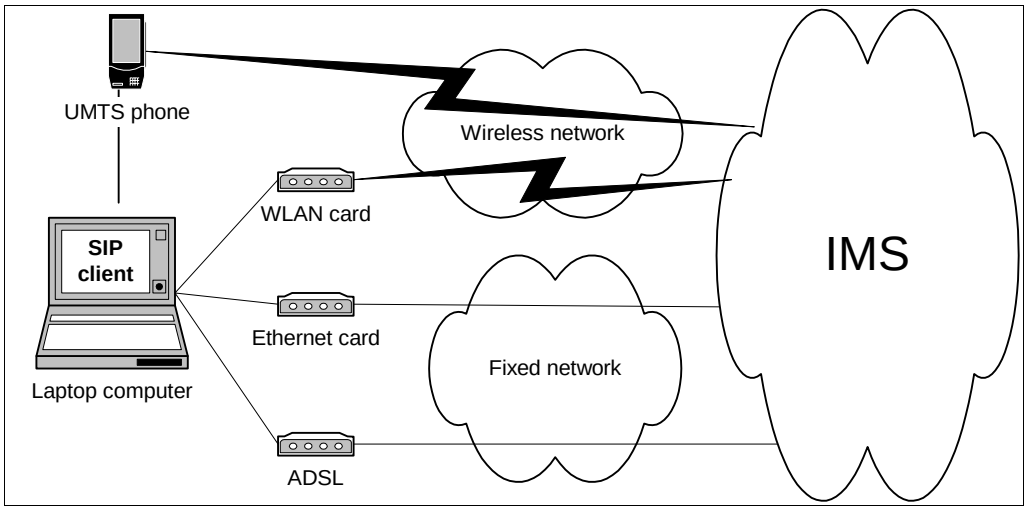

Figure 1 IMS access independence

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 to issue to achieve access independence.

In order to fulfil complete access independence, some issues have been identified and 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. In order to get access independence a user should not be forced to have a UMTS subscription, an IMS subscription should be enough.

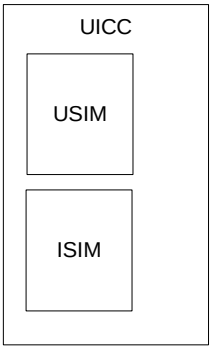

Figure 2 UICC with ISIM (and USIM)

According to the definition of ISIM, USIM and the UICC it is not possible (see definitions above). 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.

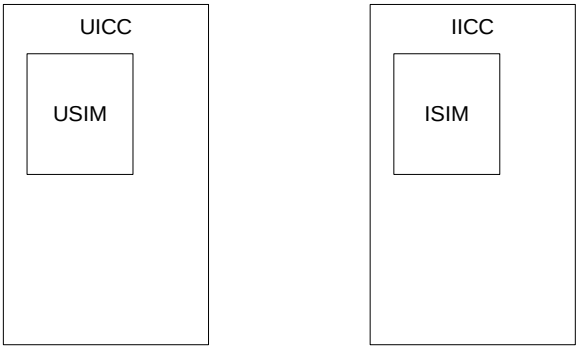

Figure 3 USIM and ISIM independence

The ISIM clearly 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 “IICC-IMS Integrated Circuit Card” that would contain the ISIM. This IICC could be the same physical card as the UICC, but not necessarily in order to get access independence. The definition of ISIM also needs to be redefined to state that the ISIM should reside on the IICC.

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. The IICC could be implemented in the same physical card as the UICC, but not necessarily ”

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 IICC.”

UE split consideration

The use of a separate ISIM on a IICC removes the problem of transferring sensitive security information over any MT – 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

The use of an ICC to store the IMS security information might also cause access independence problems from a user point of view. 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 system (operating system) does not follow a widely deployed standard a special driver is needed and this might also be a problem.

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