

27 - 30 November, 2001

Sophia Antipolis, France

3GPP TSG_SA WG2

Kobe, Japan

29/10-2/11/01

Tdoc S2-013067

Title: LS on IMS identifiers and ISIM and USIM

Source: TSG SA2

To: T3, SA3, SA1, CN1, T2

Cc: EP SCP

Contact Person:

Name: Chris Pudney
E-mail Address: chris.pudney@vf.vodafone.co.uk

1. Overall Description:

SA 2 has received the LSs from T 3 in S2-01-2743 (T3-01-0613) and from SA 3 in S2-01-2897 (S3-01-0554) and has discussed Tdoc S2-01-2818, which is attached for your information.

SA 2 note SA 3's proposal for a T 3-SA 3 workshop in Sophia Antipolis on 26/11/01. SA 2 kindly suggest that the list of invitees to the workshop should be extended to include SA 2, T 2, CN 1, and SA 1. SA 2 also believe that SA 2, T 2, T 3 and CN 1 all have meetings scheduled for 26-30/11/01 and all are in Cancun in Mexico. Unfortunately, this presents some logistical difficulties for a joint meeting with SA 3!

SA 2 believe that the issues raised in S2-01-2818 need to be discussed and resolved as quickly as possible because they may have a significant impact on the commercial success of IMS.

SA 2 suggest that participants interested in this topic and who attend SA 2, T2, T3 or CN 1 discuss this matter during the Cancun meeting. Although delegates from SA 1 and SA 3 are obviously welcome to travel to Cancun, it is likely to be more practical that they ensure that their colleagues in Cancun are well briefed on these topics.

2. Actions:

For T 3:

- a) Can T 3 confirm (or deny) the limit of 4 active applications per UICC card?
- b) Is it possible to increase this number?
- c) Can T 3 identify means to remove this restriction?

For T 2:

- a) T 2 are invited to comment on this subject, in particular with regard to UE functionality split.

For SA 1:

- a) Can SA 1 identify which service requirements prevent the reuse of R'99 USIM cards for IMS?
- b) SA 2 inform SA 1 that SA 2's network architecture is based on a single UICC in the UE. SA 2 is (as yet) unable to comment as to whether it is difficult or easy to adjust the architecture to also cater for separate UICCs in the ME and TE.

For CN 1:

- a) Can CN 1 identify the information that they are currently expecting to be stored for IMS on the UICC? (SA 2 expects that the list may include the Private User Identity; one Public User Identity; and Home Domain Name).

For SA 3:

a) Can SA 3 please comment on these issues from a security aspect?

3. Attachments:

S2-01-2818

Agenda item: Release 5: IMS

Source: Vodafone Limited

Title: **Open issues on USIMs/ISIMs/UICCs etc for IMS**

For: lots of decisions

1 Introduction

At the S2 drafting meeting in Vancouver there was some discussion about “ISIM”s and USIMs. The discussion showed that this was not merely an editorial matter within 23.228, but, had some profound service and architectural aspects.

This paper aims to provoke some discussion which can then lead to some agreements and subsequently to CRs to Release 5 specifications. Liaison statements may also need to be sent to other groups and/or some joint sessions held at future meetings.

Note: Not all of the proposals in this document represent concrete Vodafone opinions, rather, these proposals are intended to focus discussion on technical issues that need to be addressed prior to completion of Release 5.

2 UICC to ME interface

This complies to the ETSI TS 102.221 and ISO 7616-3 standards and is therefore only able to support communication for 4 (or less) “applications” simultaneously. If the user wants to use more than 4 UICC applications, the UICC applications have to be stopped and started so that, at no time, are more than 4 applications running. This is a cumbersome process and needs to be avoided.

Currently, it is imagined that mobiles could have 3 applications active (USIM, WIM (WAP identity module) and Phone Book¹). The work on “UE functionality split” may lead to the specification of another UICC application. If IMS forces the use of a standalone ISIM application, then we may need 5 applications to be active across an interface that can only support a maximum of 4 applications!

Proposal 1: the Release 5 standards shall support the means for all IMS data/algorithms on the UICC card to be accessible using the USIM application.

3 SIP application using non-3GPP access technology to connect to IMS

The access technology might, for example, be Wireless LAN. It is believed that the proponents of “access independence” to IMS do not want to force every IMS terminal to have a USIM. Although there does not appear to be any technical problem with mandating the use of a USIM, there may be minor operational issues.

Question 2: Is access independence seen as vital for 3GPP Release 5? (ie is access independence permitted to delay Release 5?)

¹ The use of a separate Phone Book application allows faster phone book extraction.

Proposal 3: if (and only if) access independence is seen as vital for 3GPP Release 5, the Release 5 standards should support means for IMS data/algorithms on the UICC card to be accessible through non-USIM UICC applications.

4 Dis-integrated terminal: access to UICC in the ME

This could be the case of a laptop or PDA using a mobile to access the IMS. The laptop/PDA is using the UICC card in the mobile to provide authentication of the IMS sessions.

This case is believed to be one of the main drivers for the work on the “UE functional split” feature. Owing to its late start, it is unclear whether or not this feature will be part of Release 5.

Proposal 4: the work on “UE functional split” should facilitate access to any IMS data/algorithms stored on the UICC card.

5 Dis-integrated terminal: separate UICCs in TE and ME

Corridor discussion at the S2 drafting meetings in Vancouver raised this possibility.

Question 5: will this delay Release 5, or, would it permit faster trialing and debugging of Release 5?

Question 6: does this have any real architectural impact (eg what if the two UICC cards come from different HSSs/different PLMNs), or, can this matter be left to the security experts in SA 3?

Proposal 7: If this is permitted, then it shall be possible to use a USIM in the TE.

Proposal 8: If this is permitted, then any IMS emergency call handling may need to be updated to handle all combinations of TE and ME with/without UICC cards.

6 Reuse of unmodified USIM

One of the successes of GPRS has been that it is possible to use GPRS mobiles with unmodified SIM cards. It seems sensible to ensure that something similar can be done for IMS, namely that [integrated] IMS mobiles can work with an unmodified R’99 USIM.

In order to achieve this, it seems likely that, for non-IMS UICC cards, the main requirement is to specify a rule which the ME [and CSCFs] can use for producing the Private User Identity from the IMSI.

Proposal 9: the Release 5 standard shall include means by which a UE can run IMS services with one unmodified R’99 USIM and without (significantly) degraded security.

7 Conclusion

These matters should be discussed and resolved as a matter of urgency.