3GPP TSG-SA3 Meeting #21 ***Tdoc S3-010625***
Sophia Antipolis, France, 26 - 30 November 2001

Source: Ericsson

Title: Use of a R99 or REL-4 USIM application on a UICC card for IMS services

Agenda item: Joint Meeting with T3

Document for: Discussion

1 Introduction

This contribution addresses the issues related to the use of a R99 or a REL-4 USIM application on a UICC card for IMS services. This discussion was initiated at SA2 #20 in Kobe, Japan (communicated to S3 in LS S3-010576) and will be further discussed in SA2 #21 in Cancun.

When GPRS was introduced in R97, the operators wanted to be able to re-use the old GSM SIM cards already on the market, for GPRS services, in order to avoid having to distribute new SIM cards with GPRS support.

This contribution presents Ericsson’s findings while analysing the proposal. This paper seeks for discussion at S3 in order to settle some basis for further work on this matter.

2 Discussion

This section describes some assumptions Ericsson would like to discuss in order to seek a common understanding, and also some open issues, which need to be discussed in order to find a solution.

In order to resolve the case when a R99 or REL-4 UICC card is inserted in a UE, the issues mentioned in this paper will not have any impacts on the signalling protocol or the network behaviour, unless it’s decided to perform some kind of optimisation in the network to resolve the synchronisation failures discussed in bullet 7 in chapter 2.2.

In order to allow a MT to gain access to IMS the network will send an authentication request with a RAND and AUTN to the MT. Since there will be no ISIM application available at the UICC, the MT will pass the authentication request on to the USIM application and the USIM application will respond with a RES together with the security keys to the MT.

2.1 Assumptions

If the MT concludes that the UICC card does not contain any support for IMS services then:

1. The MT shall re-use the USIM application on the UICC for IMS services in order to perform authentication and retrieval of security keys for IMS services.

2. The integrity key (IK) and encryption key (CK) provided from the USIM application shall be used by the MT for integrity protection and encryption of IMS signaling, if encryption is supported. The MT does not need to perform any conversion of the keys.

3. The MT shall not store the security keys for IMS services on the USIM application, in order to avoid overwriting the existing security keys for GPRS. The security keys for IMS services shall be stored in the MT.

4. As authentication is mandatory when the MS performs the initial registration for IMS services, there is no need to store the security keys for IMS services in the MT at power off.

5. In TS 23.228 REL-5 in S2, there is currently a request to store at least one IMPU on the UICC card. If this requirement stays in REL-5, then the MT shall be able to store at least one IMPU, which shall be stored in the MT at power off. It is assumed that the IMPU in this case will be introduced manually by the user to the MT.

6. The MT shall store the IMPI and the Home Network Name in the MT at power off. It is assumed that Home Network Name will be introduced manually by the user to the MT. Refer to discussion in bullet 9) related to how IMPI could be handled.

7. In TS 24.008 R99 a new requirement was introduced in the Mobility Management layer to store the last received RAND as well as the corresponding RES, CK and IK. When the MT received an Authentication Request, the MT had to check whether the RAND was repeated in order to detect re-transmissions from the network and avoid re-synchronization failures on the USIM application as the USIM application could not handle duplicated requests. In addition, new guard timers were introduced in the Mobility Management layer, which controlled how long the ME had to store the RAND and the corresponding RES, CK and IK. It is proposed that the same handling is introduced in the IMS client.

2.2 Open issues

In addition we would like to address some issues as:

8. The number of synchronization failures on the USIM application might increase as a cause of using the same USIM application for authentication of CS, GPRS and IMS services. This would imply some extra IMS and GPRS signalling in order to resolve the synchronization failures by performing re-synchronization in the network. In addition, a new authentication vector (or batch of Avs) will be retrieved at each re-synchronization.

    a. If the potential increase in the number of synchronisation failures is not considered to be a major problem, then the already existing procedure in TS 33.102 defined in the network to perform re-synchronisation will resolve the synchronisation failures.

    b. We might have to consider whether any additional optimisation, e.g. distribute only one authentication vector to the S-SCSF at a request, or the use of specific SQN management schemes could help to decrease the signaling and minimise the number of synchronisation failures on the USIM application.

    NOTE: According to TS 24.008, in GPRS, the MS shall bar the current serving cell in the case when authentication has subsequently failed a second time.

9. As a R99 or REL-4 USIM application on a UICC card does not contain any IMS related parameters as IMPI, we need to define how the MT shall handle the IMPI.

    - One of the potential solutions could be that the MT creates and stores the IMPI in the following format: IMSI@HomeNetworkDomain, where the IMSI is retrieved from the UICC card and the ‘Home Network Domain’ is manually entered by the user.

      The IMPI shall be stored in the MT at power off. At power on the MT shall compare the IMSI part of IMPI stored in the MT with the IMSI stored on the SIM card in order to find out whether a new SIM card has been inserted into the UE. If a new SIM card has been inserted, then the MT shall delete the IMPI and the Home Network Domain stored in the MT.

      NOTE: One has to consider that IMPI based on IMSI and particularly in this case where the IMPI (IMSI) would be stored in the MT, open up for a new security threat to UMTS where IMSI confidentiality would be exposed.

    - An alternative could also be that the user enters the complete IMPI into the MT (this will enable the use of IMPIs not based on IMSI).

10. It needs to be considered how the case shall be handled when an old GSM SIM card is inserted in the UE and the user attempts to register for IMS services.

3 Proposal

Ericsson proposes to discuss the above addressed assumptions in order to reach a common understanding and attempt to resolve the open issues. Additionally, it should be identified the appropriate way to address these issues in 3GPP standards so minimum impact on current architectural principles is achieved.