3GPP TSG-SA3 Meeting #21 ***Tdoc S3-010624***
Sophia Antipolis, France, 26-30 November 2001

Source:	Ericsson
Title:	Parameters stored on a UICC card for IMS services
Agenda item:	Joint meeting with T3
Document for:	Discussion

1 Introduction

This contribution discusses the parameters and functionality that needs to be stored on a UICC card for IMS services.

2 Discussion

This section discusses different parameters specified in TS 33.203 and TS 33.102.

2.1 IM Private Identity (IMPI)

The IMPI is the user's private identity, which is used by the network to authenticate the subscriber. For security reasons the IMPI shall be stored on the UICC.

2.2 IM Public Identity (IMPU)

According to TS 23.228 at least one IMPU shall be stored on the UICC. From security point of view there is no need to store the IMPU on the UICC card, but it could be useful to limit the necessary configuration.

2.3 Key set identifier for IMS (KSI)

The need for KSI for IMS in SIP signalling is still an open issue in TS 33.203 and needs to be further investigated by S3.

2.4 Security keys for integrity protection and encryption (IK & CK)

The storing of the security keys at UICC is related to the discussion regarding the need for KSI for IMS, which needs to be further investigated by S3.

2.5 Algorithms

The same framework should apply for the ISIM application as for the USIM application. Whether the same or different algorithms shall be used by the ISIM and USIM application is an operator choice.

2.6 Home Network Domain name

The Home Network Domain name needs to be stored on the UICC in order to make it possible for the UE to register in its home network.

2.7 Others

2.7.1 SQN

To be able to have a separate SQN handling in the network for CS, GPRS and IMS in order to avoid synchronization failures on the ISIM and USIM applications, the ISIM application should have it’s own SQN management scheme.

2.7.2 AMF

How the AMF is used in the network and on the ISIM application is an operator choice.

2.7.3 START value

There is no need to use any START values or any related parameters as HFN and THRESHOLD for integrity protection of IMS signaling, i.e. there is no need to store THRESHOLD and HFN on the UICC card.

2.7.4 K (authentication key)

The same key or different keys could be used by the USIM application and the ISIM application on a UICC.

3 Summary

According to current requirements in TS33.102, TS33.203 and TS23.228, it is considered that the following information shall be stored by the IMS application in the UICC (ISIM) …

- IMPI
- Home Network Domain name
- New SQN management scheme
- Algorithms and authentication key (K)

Additionally, ISIM may have also to store the following information, but it shall be further study whether this is really required…

- KSI for IMS and security keys
- AMF

S3/T3 should ask S2 whether the requirement to store at least one IMPU on the UICC card shall be kept, even though S3 from a security point of view don’t see the need.

In addition, it is proposed to consider for further investigation how the ISIM and USIM applications could share the following information...

- same algorithms and authentication key (K)
- SQN Management scheme
- AMF (if required for IMS).