3GPP TSG SA WG3 Security — S3#20 **S3-010584**

27 - 30 November, 2001

Sophia Antipolis, France

From: **Jeremy Norris (Vodafone Ltd) USIM rapporteur**

Subject: **T3 ISIM working assumptions**

T3 has made the attached document on the its working assumptions on the subscription for the IMS subscription.

3GPP-T WG3: IMS working assumptions

Rapporteur : Jeremy M Norris

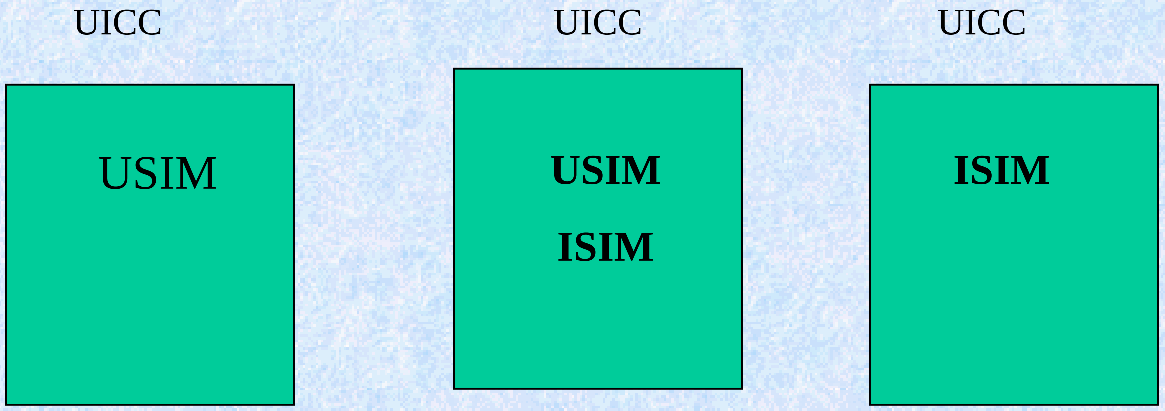
AIM:

The aim of this presentation is to describe T3’s working assumptions when designing the subscriber identity module for support of IMS.

This information is based on the input received from S3, S1 and S2 on the subject.

The aim of this document is to present T3’s assumptions to the respective workgroups so a common understanding exists, and to ensure all the requirements are taken into account.

UICC Architecture Alternatives



•**Use case 1a** - R’99 USIM - No IMS data stored on the card. All IMS information is derived by the terminal from existing information stored on the card. IMS security parameters obtained with existing R’99 AKA sequence.

•**Use case 1b** - R’5 USIM - IMS data stored on the card. IMS security parameters obtained with existing R’99 AKA sequence.

•**Use case 2** - USIM+ISIM - All IMS subscription is held in the ISIM application. Data can be shared between applications, but this is up to the operator to specify.

•**Use case 3** - ISIM only - For IMS only providers. As a result there is no need for them to provision the USIM.

Use case 1a: R’99 USIM

AIM: To allow existing 3G cards to be reused. Avoids different card types in the supply chain.

Advantages:

- USIM cards can be used for access to IMS without re-issuing the cards. Easier for the terminal manufacturers to provide support for IMS for initial releases of IMS capable terminals.
- Time to market reduced due to reduced cost and minimising of the changes to the network.
- Avoids IOT problems caused by “ISIMs” having to be rolled out long before IMS capable terminals are available.

Disadvantages

- Subscription not logically separate.

Technical issues:

- Lifetime of the integrity/ciphering keys for the IMS subscription i.e the hyper-frame number is used in 3G what will be used in IMS to control the lifetime of the keys?
- Interleaving of the Sequence numbers.
- Formulation of the private identity and home domain name from the IMSI. Formulation of the public identity from the MSISDN

Use case 1b: Release 5 USIM

AIM: Minimise existing changes to tested/debugged USIMs. Avoid shortage of logical channels on terminal to card interface.

Advantages:

- USIM cards can be used for access to IMS without re-issuing the cards. Easier for the terminal manufacturers to provide support for IMS for initial releases of IMS capable terminals.
- Time to market reduced due to reduced cost and minimising of the changes to the network.
- Private identity, home domain name and public identity stored on USIM.

Disadvantages

- subscription not logically separate.

Technical issues:

- Lifetime of the integrity/ciphering keys for the IMS subscription (as case 1a)
- Interleaving of the Sequence numbers.

- New IMS fields on USIM might be provided by OTA.

Use case 2: UICC with USIM and ISIM

AIM: New cards with revised AuC and HLR.

Advantages:

- Logically separate subscription.
- No reliance on the mobile to store the information meaning the data is interchangeable due to the UICC being removable. All subscription related information stored on the card and no need to derive the information from the USIM subscription.

Disadvantages:

- Use of a logical channel and use of a resource whilst the subscription is active.
- Additional memory usage of the card . This may be an issue for an operator who already has multiple applications on the card.
- ISIM application [cannot] be reliably provided by OTA.

Technical issues:

- Lifetime of the integrity/ciphering keys for the IMS subscription (as case 1)
- The terminal will need to start the card’s IMS application even if there is no IMS service available.
- Authentication algorithm parameters and sequence numbers might be shared.

Use case 3: ISIM only

Aim: Separate subscription from the RAT? E.g. connection to a wireless LAN.

Advantages:

- Logically separate subscription.
- Independent of the RAT bearer.

- **Disadvantages:**
- Subscription for RAT held elsewhere.
- Dual slot terminals may be required, as the bearer subscription may be held elsewhere.
- Customer confusion (e.g. how can a user tell the difference between an UICC holding an ISIM application and an UICC holding an USIM application?).

Technical issues:

- Lifetime of the integrity/ciphering keys for the IMS subscription (as case 1)
- Can the IMS architecture support ISIM and USIM from different HSSs/PLMNs (e.g. in different countries?).

3GPP WG3 T3 specifications

Proposed WI output.

- ISIM specification TR 3X.XXX, much like TR 31.900 “SIM/USIM Internal and External Interworking Aspects”.
- Inter-working document for subscription for IMS access.
  - Consideration of dual application card holding an ISIM and USIM with respect to authentication parameter sharing.
  - Consideration of a R’99 subscription holding an USIM application.