3GPP TSG SA WG3 #21bis aSIP ad hoc **Tdoc S3z020033**
Antwerp, Belgium
31st January – 1st February 2002

3GPP T3 (USIM) Meeting #22 ***Tdoc T3-020139***
Marbella, Spain, 22 - 25 January 2002

Title: **Liaison Statement on ISIM for support of IMS**

Source: **T3**

To: **SA1, SA3**

cc: **T2, SA2**

Contact Person: Jeremy Norris

E-mail Address: jeremy.norris@Vodafone.co.uk
Tel. Number: +44 1635 673395

Attachment: T3-020140 "ISIM working assumptions"

---

1. Introduction:

T3 have been discussing the support of IMS services, known as ISIM, on the UICC. As a result T3 have reached a set of working assumptions as described in the attached presentation. T3 have identified two issues that T3 believe SA1 need to review.

2. Description:

a) With the use cases identified by T3, it would be possible to have more than one IMS subscription active at any one time, possibly from different IMS service providers. From a technical point of view, the UICC is currently able support up to four simultaneously active applications. SA1 and SA3 are requested to confirm this requirement.

b) Other assumptions are outlined in the attached presentation. SA1 and SA3 are requested to review these assumptions and provide feedback to T3.

3. Actions:

see descriptions above

4. Date of Next T3 Meetings:

T3 ad hoc on ISIM issues	19 - 21 March (to be confirmed), Sophia Antipolis or Newbury
T3 meeting #23	21-24 May, Finland

Tdoc T3-020140

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 SA3, SA1,CN1 and SA2 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.

Requirements

CN1 Requirements as described in their LS from CN1 #20bis (T3-020006/N1-011768)

- **Private User Identity** - it is assumed that this is stored on the UICC, although for access independence it may be possible for the operator to provide the user with some other means of entering the private ID.
- **Public User Identity** - it is assumed that (as per TS 23.228) at least one public identity will be stored on the UICC. It is CN1's opinion that public IDs could also be stored in the user equipment or be entered by the user.
- **Alias** - CN1 assumes that it may be possible for the user to enter an alias e.g. to be displayed as a CLI or dial-back number.
- **Cell ID** - This field shall only be obtained from the user equipment.
- Visited Network Identifier - The assumption is that this field will be inserted by the P-CSCF.
- **Home Network Domain** - It is assumed that this field will be stored on the UICC.
- **Event packages** - It may be necessary for a terminal to have access to certain events to which it must subscribe. It is currently assumed that this information will be stored in the user equipment

- **Security Keys/Algorithms -** CN1 has not yet considered where this information will be stored and awaits input from SA3, although it is envisaged that the UICC may be impacted.

S3 Requirements (S3-010647/T3-0200008 from SA3 #21 and T3-0200040 (draft (v0.0.5) report from joint SA3/T3 meeting, 26th Nov)

- Related to this document Use Cases 2 and 3 were agreed as necessary (these cases are equivalent from a T WG3 viewpoint). Use Case 1b was considered by T WG3 viewpoint to be very close to Use Case 2.
- "Middle case" using OTA to update pre-Rel-5 cards was also identified during the meeting. If Either Use Case 1a OR the "Middle Case", or neither of these two, should be supported. Some of CN WG1 assumptions need to be removed if Use Case 1a is adopted.
- User should not be able to modify/enter the IMPI or Home Domain Name due to user-friendliness, erroneous entry of IDs and DoS attack potential.
- The Parameters that SHALL be included in the ISIM application (Security reasons) and those which may be best included in the ISIM application for other reasons to be identified.

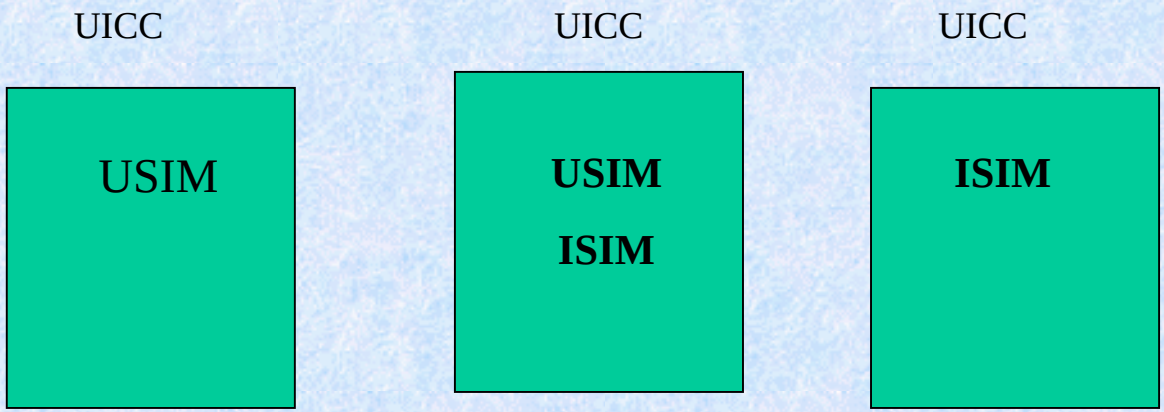
  SHALL be in ISIM application: IMPI; Home Network Domain Name; Support for SQN used in the context of IMS domain; Algorithms and Authentication Key (K).

- FOR FURTHER STUDY (Depends on the final mechanisms for protecting SIP signalling): Security Keys (CK, IK); KSI, equivalent to the START parameter; AMF related data.
- Identified Issues with Use Case 1a: Potential increased signalling due to re-synchronisations; Derivation of Private ID from the IMSI / Protection of IMSI from eavesdropping; Increased potential for DoS attacks; Lack of Public Identity - MSISDN not compulsory in the USIM so cannot always derive IMPU from this. Some initial solutions were proposed and discussed.
- NON-SECURITY RELATED ISSUES: "plastic" roaming, i.e. support for changing the terminal; Cost of supported features in terminals; Cost of OTA provisioning; Cost of re-issue of cards and management of card distribution; restrictions on further developments of IMS Security Architecture and IMS in general; Number of options to be supported in general.
- There is no requirement that the algorithms and master keys shall be different.

TSG-SA (T3-020024, Draft Report for TSG SA meeting #14 v0.0.3)

- It was agreed that the platform where the IMS security parameters and access functions would reside is the UICC (rather than on the terminal, etc.). It was proposed that the ISIM should be considered as a logical set of fields within the UICC in order to provide access to 3GPP Core Network, allowing IMS to be secured in the Rel-5 time frame. This would not preclude future separation of the functionality.
- It was agreed that so far, "ISIM" denotes the subscription information and security functions required for IMS. It is believed that that ISIM functionality is essential for Rel-5 in order to make IMS functional. WGs with requirements for ISIM were asked to specify these urgently to T WG3. It is the preference of TSG SA that T WG3 specify a solution that does not preclude that, in future Releases, the IMS subscription could be independent from the basic subscription currently stored in the USIM.

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 (InterOperability Tests) 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:

- USIMs 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?).

Proposed WI output and conclusions.

Conclusions

- Case 1A is not considered practical to implement and noting CN1 requirements for fields stored in the card, not applicable.
- For Rel-5 the other cases of 1b,2/3 will be considered by T3.
- The encapsulated document describes the various file combinations of ISIM/USIM identified by T3:

Microsoft
werPoint Presentati

Output

- ISIM specification TS 31.103. This will consider a separate application and files within the USIM application for IMS access. The USIM specification will refer to this specification for use case 1b.