3GPP TSG SA WG3 Security — S3#21 **S3-010642**

27-30 November, 2001

Sophia Antipolis, France

Source: **S3**

To: **T3, SA2, SA1, CN1, T2**

Cc: **EP SCP**

Title: **Draft Response** LS on **IMS identifiers and ISIM and USIM**

Contact: **valtteri.niemi@nokia.com**

Attachments: S3-010584; S3-010580

SA3 and T3 had a joint ad hoc meeting on ISIM issues 26th November 2001. During the meeting the following LSs were discussed:

S2-013067 on IMS identifiers and ISIM and USIM;

N1-011768 on IMS identifiers;

T3-010730 on the same subject also.

Some of the conclusions of the joint meeting are listed in the following (I - VI).

I. Related to S3-010584: The document presented T3 working assumptions on ISIM. Different use cases were identified:

"

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 Cases 2 and 3 were agreed as necessary. These two cases are also equivalent from a T WG3 (or UICC specification) viewpoint. Use Case 1b was considered by T WG3 viewpoint to be very close to Use Case 2.

During the discussion a "Middle case" using OTA to update (any release) UICCs was mentioned.

It was concluded that either Use Case 1a OR the "Middle Case", or neither of these two, should be supported. Some of CN WG1 assumptions listed in N1-011768 need to be removed if Use Case 1a is adopted.

II. Several open questions were raised in S3-010580 as follows. The conclusions of the joint meeting are in bold-face.

"

1 *In TS 33.203 the ISIM is responsible for handling the keys etc. tailored to the IM CN SS. In TS 23.228 and TS 24.228 however, the USIM seems to be given this role. In S2, there are discussions going on about access independence for IMS and thus defining an ISIM independent from the USIM.*
It is most likely that this latter option will be chosen.
The meeting agreed that this should be ISIM - i.e. 23.228 and 24.228 should be updated.

2 *A Service profile is attached to one or more public ID's and to one Private ID. In the case of access independence, i.e. obtaining access to the same service via different terminals, each with an ISIM, these ISIMs should bare the same private Identity. Is this allowed?*
The meeting agreed that this should not be allowed; for each Private Identity there should be only one ISIM.

3 *It is not defined yet if the algorithms and keys used for IMS are different than the ones defined in the USIM*
There is no requirement that the algorithms and master keys shall be different. On the other hand, there is no requirement that they shall be the same. The matter is up to the operator.

4 *Are there other functions that can be allocated to the ISIM, like phonebook, 'call control', operator preferences, ISIM Application Toolkit, generation of Call-ID, etc.?*
From the SA WG3 point of view, there is no position on this. This should be raised in other groups to see if there are any requirements for this.

"

III Related to the use case 1a (see above) there was a discussion about the IMS data derived in the terminal. It was concluded:

User should not be able to modify/enter the IMPI (i.e. Private ID) or Home Network Domain name due to issues around user-friendliness, possibility of erroneous entry of IDs and "Denial of Service" attack potential.

IV The joint meeting discussed parameters that SHALL be included in the ISIM application because of security reasons and those which may be best included in the ISIM application for other reasons. The meeting concluded that:

ISIM application SHALL include (at least) the following: **IMPI; Home Network Domain Name; Support for SQNs used in the context of IMS domain; Algorithms and Authentication Key (K).**

FOR FURTHER STUDY (Depends on the final decision on the mechanisms for protecting SIP signalling): Security Keys (CK, IK); data equivalent to the Key Set Identifier; data equivalent to the START parameter; AMF related data.

V The meeting discussed issues with Use Case 1a. The identified issues are listed in the following. Some initial solutions were also proposed and discussed.

Potentially increased signalling load due to re-synchronisations of SQNs;

Derivation of Private user ID (IMPI) from the IMSI;

Protection of IMSI from eavesdropping (user identity confidentiality);

Increased potential for DoS attacks;

Derivation of Public User Identity (IMPU)- MSISDN is not compulsory in the USIM; so cannot always derive IMPU from it.

VI Some NON-security related issues were also identified during the meeting:

With Use case 1a : "plastic" roaming, i.e. support for changing the terminal; restrictions implied on further developments of IMS Security Architecture and IMS in general

With all Use cases: Cost issues, including cost of supported features in terminals, cost of OTA provisioning, Cost of re-issuing of cards and management of card distribution;

With all use cases Number of options to be supported in general.

ACTIONS:

SA2 and CN1: To update specs 23.228 and 24.228 according to the findings in II.

CN1: To study the effects of I on working assumptions of CN1

All groups: To study non-security related issues referred to in II and VI.