3GPP TSG SA WG3 Security — S3#22 **S3-020109**

25 - 28 February 2002

Bristol, UK

Source:	Vodafone
Title:	Proposed changes to 33.203 v1.1.0 regarding ISIM
Document for:	Approval
Agenda Item:	

Some changes are proposed to 33.203 to take into account recent decisions made in SA1 and SA2.

Section 3.1: The USIM definition conflicts with the definition in 21.905, so it is deleted. The ISIM definition is updated.

Section 4: Introductory text on the ISIM is updated. A reference to section 8 is included.

Section 8: Detailed text on the ISIM is updated. In particular, text is added regarding the use of a USIM for accessing IMS services. This text based on a Vodafone contribution to SA3#21 (S3-010641).

3.1 Definitions

For the purposes of the present document, the following terms and definitions apply.

Authenticated (re-) registration: A registration i.e. a SIP register is sent towards the Home Network which will trigger a authentication of the IMS subscriber i.e. a challenge is generated and sent to the UE.

Confidentiality: The property that information is not made available or disclosed to unauthorised individuals, entities or processes.

Data integrity: The property that data has not been altered in an unauthorised manner.

Data origin authentication: The corroboration that the source of data received is as claimed.

Entity authentication: The provision of assurance of the claimed identity of an entity.

Key freshness: A key is fresh if it can be guaranteed to be new, as opposed to an old key being reused through actions of either an adversary or authorised party.

~~**USIM – User Services Identity Module.** In a security context, this module is responsible for performing UMTS subscriber and network authentication and key agreement. It should also be capable of performing GSM authentication and key agreement to enable the subscriber to roam easily into a GSM Radio Access Network.~~

ISIM – IM Services Identity Module. For the purposes of this document the ISIM is a term that indicates the collection of IMS security data and functions on the UICC. The ISIM may be a distinct application on the UICC. ~~In a security context, this module is responsible for performing subscriber and network authentication and key agreement in IMS. The ISIM resides on the UICC~~.

4 Overview of the security architecture

In the PS domain, the service is not provided until a security association is established between the mobile equipment and the network. IMS is essentially an overlay to the PS-Domain and has a low dependency of the PS-domain. Consequently a separate security association is required between the multimedia client and the IMS before access is granted to multimedia services. The IMS Security Architecture is shown in the following figure. ~~The ISIM is responsible for the handling of keys, SQN etc that are tailored to IMS. The security parameters handled by the ISIM are independent of the similar security parameters that exist in the USIM.~~

IMS authentication keys and functions at the user side shall be stored on the UICC. It shall be possible for the IMS authentication keys and functions to be logically independent to the keys and functions used for PS domain authentication. However, this does not preclude common authentication keys and functions from being used for IMS and PS domain authentication.

For the purposes of this document the ISIM is a term that indicates the collection of IMS security data and functions on the UICC. Further information on the ISIM is given in section 8.

~~Although ISIM and USIM are logically independent, all the following cases are possible for implementation:~~

~~- ISIM and USIM are implemented as a single application inside one UICC~~
~~- ISIM and USIM are implemented as two distinct applications inside one UICC~~
- ~~ISIM and USIM are implemented inside two distinct UICCs.~~

8 ISIM

~~The ISIM is logically independent from the USIM to represent the IMS subscription and its associated data. It is necessary for this subscription information to be independent of the corresponding USIM data to support access network independence. Furthermore the IMPI, the Home Network Domain Name and at least one IMPU shall be securely stored on the UICC i.e. the logically separate ISIM. The ISIM and USIM may be implemented on the same UICC, and may be provisioned by the same provider. Although ISIM and USIM are logically independent, all the following cases are possible for implementation:~~

~~- ISIM and USIM are implemented as a single application inside one UICC~~
~~- ISIM and USIM are implemented as two distinct applications inside one UICC~~
~~- ISIM and USIM are implemented inside two distinct UICCs.~~

For the purposes of this document the ISIM is a term that indicates the collection of IMS security data and functions on the UICC. The following implementation options shall be permitted:

- Use of a distinct ISIM application on a UICC which does not share security functions with the USIM;
- Use of a distinct ISIM application on a UICC which does share security functions with the USIM;
- Use of a R99/Rel-4 USIM application on a UICC.

~~*[Editors Note: It is FFS if and how a R'99 and R'4 USIM can be reused for IMS. Open issues related to this are:*~~

~~*- Increased signaling load due to re-synchronization's*~~
~~*- Derivation of the IMPI from the IMSI*~~
~~*- Protection of IMSI from eavesdropping i.e. user identity confidentiality*~~
~~*- Derivation of IMPUs. Note that MSISDN is not compulsory in the USIM so the IMPU can not always be derived from that*~~
~~*- Which scenario to support i.e. R'99 USIM and no IMS data is stored on the UICC or R'5 USIM and IMS data is stored on the UICC and IMS security parameters are derived with existing R'99 AKA sequence]*~~

There shall only be one ISIM or USIM for each IMPI. ~~The USIM and the ISIM may share the same algorithms and the same long-term key. It is an operator choice if the long-term key and the algorithms are different.~~ The IMS subscriber shall not be able to modify or enter the IMPI. The IMS subscriber shall not be able to modify or enter the Home Domain Name.

8.1 Requirements on the ISIM application

This section identifies requirements on the ISIM application to support IMS access security. It does not identify any data or functions that may be required on the ISIM application for non-security purposes.

The ISIM shall include:

- The IMPI
- At least one IMPU
- Home Network Domain Name
- Support for ~~SQN~~ sequence number checking~~used~~ in the context of the IMS Domain
- The same framework for algorithms as specified for the USIM applies for the ISIM
- An Authentication Key

The ISIM shall deliver the CK to the UE although it is not required that SIP signaling is confidentiality protected.

[Editors Note: It is FFS if a KSI, data equivalent to the START parameter, AMF related data, storage for CK and IK is needed or not.]

[Editors Note: It is FFS if an IMS subscriber shall be de-registered at power off]

8.2 Sharing security functions and data with the USIM

When an ISIM is used for IMS access, the following options for sharing security functions and data shall be permitted:

- No security functions or data are shared;
- The authentication key, authentication functions and the sequence number checking are shared.

It shall be explicitly forbidden to share the authentication key and functions, but to use independent sequence number checking mechanisms.

When a USIM is used for IMS access, only the following option is applicable:

- The authentication key, authentication functions and the sequence number checking are shared

8.2.1 Authentication keys and functions

If the same authentication keys and functions are shared, the cipher/integrity key sets generated during authentication are used with different cipher/integrity algorithms in UMTS and IMS. The same cipher/integrity key set is never used for both UMTS and IMS because the authentication and key agreement protocol is run independently within each domain. Therefore there is no danger that the compromise of the cipher/integrity algorithm in one domain would lead to vulnerabilities in the other domain.

8.2.2 Sequence number checking

If the mechanism and data for checking sequence numbers are shared then it shall be required for the authentication failure rate due to synchronisation failures to be kept sufficiently low. In particular, the mechanism shall be required to support interleaving authentication in three domains (CS, PS and IMS).

The example sequence number management schemes in 3G TS 33.102 Informative Annex C can be used to ensure that the authentication failure rate due to synchronisation failures to kept sufficiently low when the sequence number mechanism and data is shared between the UMTS and IMS domains. For instance, the method for the allocation of index values in the AuC, which is described in Annex C.3.4 of 3G TS 33.102, could be enhanced so that authentication vectors distributed to different service domains shall always have different index values (i.e. separate ranges of index values are reserved for PS, CS and IMS operation). This would require the AuC to obtain information about which type of service node requested the authentication vectors. As the possibility for out of order use of authentication vectors within the IMS service domain may be quite low, the number of PS or CS array elements that need to be reallocated to the IMS domain could be quite small so that the ability to support out of order authentication vectors within the PS and CS domains is not adversely affected. Reallocation of array elements to the IMS domain can be done in the AuC with no changes required to already deployed USIMs.

8.3 Other implications of using a USIM for IMS access

If a USIM is used for IMS access, the UE shall derive an IMPI and Home Domain Name in the correct format from the IMSI stored in the USIM. The derivation function shall be reversible to allow the HSS to use the IMSI as the basis for indexing the correct record in the AuC without having to maintain a large look-up table. The derivation function shall be standardized in the UE so that the HSS can use the same mechanism for deriving the IMSI. A reversible function has the potential disadvantage that anyone who obtains IMS identification parameters can determine the corresponding IMSI. However, this is not assumed to be a problem in scenarios where a USIM is used for providing IMS access.

If a USIM is used for IMS access, the IMS public identities shall be stored on the UE rather than on the UICC.

Editor's note: If a USIM is used for IMS access, any IMS-specific integrity keys, cipher keys, key identifiers, key lifetimes, counter values, etc. (more generally the IMS security association) would need to be stored on the UE. The exact content of the IMS security association is ffs. Storage of the IMS security assocation on the UE would limit the ability to move the UICC between different UEs without having to re-authenticate each time. It also means that the keys shall be stored in the UE at power off rather than on the UICC. However, this is considered no worse that the storage of GPRS cipher keys on the UE when a non-GPRS aware SIM is used.