3GPP TSG SA WG3 Security — S3#20 **S3-010641**

27 - 30 November, 2001

Sophia Antipolis, France

Agenda Item: Joint meeting with T3

Source: Vodafone

Title: On the use of R99/Rel-4 USIMs for IMS access

Document for: Discussion and decision

1 Introduction

As progress is made to define a security architecture for IMS, it is timely to consider how the security critical functions at the user end might be realised. IMS access security is based on the use of the UMTS authentication and key agreement protocol. Therefore the necessary security functions at the user side are already supported by the USIM. In this contribution we consider whether it would be possible, as an option, to use a R99 or Rel-4 USIM application on a UICC for IMS access security. We consider the case where the UMTS and IMS operators coincide such that a common authentication key and algorithm on the USIM and a common AuC in the network can be used for both IMS and UMTS access security.

2 Discussion

A number of issues have been identified which impact whether or not it would be possible to use a R99 or Rel-4 USIM application for providing IMS security. These issues are discussed below.

2.1 Sequence number management

In UMTS the sequence number management scheme for network authentication must keep the number of synchronization failures due to interleaving authentication in the PS and CS domains to an acceptable level. If the USIM is also used for IMS access security then interleaving authentication with a third domain must also be supported. This will result in a potential increase in the number of synchronization failures which will have a corresponding impact on network signaling load, authentication vector consumption and authentication delay.

The sequence number management schemes in 33.102 Informative Annex C can eliminate the possibility of synchronization failures due to interleaving authentication in multiple domains if the AuC can allocate index values in the array based on the identity of the domain which originated the authentication vector request. This is done by reserving specific index values (corresponding to array elements on the USIM) for each domain. If an extra domain is introduced for IMS, fewer array elements will be available for each domain. As a consequence there will be a potential increase in the occurrence of synchronization failures due to out of order use of authentication vectors within a particular domain. However, the possibility for out of order use of authentication vectors within the IMS may be quite low compared to the CS and PS domain. Therefore the number of PS or CS array elements that need to be re-allocated to the IMS domain could be quite small such that the ability to support out of order authentication vectors within the PS and CS domains is not adversely affected.

Note that the re-allocation of array elements to the IMS domain could be done in the AuC with no changes required to already deployed USIMs.

2.2 IMS private identity and home domain name

If a R99 USIM is used, the terminal could derive an IMS private id and home domain name in the correct format from the IMSI. Although the exact rules for deriving the IMS private id and home domain name are ffs, two cases exist depending on whether or not the derivation function is reversible, i.e. whether or not the IMSI can be derived from the corresponding IMS private id and home domain name.

A reversible function would allow an HSS to derive the IMSI from the corresponding IMS identification parameters and use it as the basis for indexing the correct record in the AuC. If an irreversible function were used then it necessary to modify the AuC so that it can be indexed using both the IMSI and the IMS identification parameters. A reversible function has the disadvantage that anyone who obtains IMS identification parameters can determine the corresponding IMSI. This may be an issue if the IMS identification parameters are distributed outside the UMTS operator’s domain since it may be undesirable to reveal IMSIs outside the UMTS network. However, if a USIM is used for IMS access it is assumed that the UMTS and IMS operators coincide. Therefore we conclude that a reversible function is acceptable from a security perspective. If a reversible function is used then it must be standardized in all terminals so that the HSS can use the same mechanism for deriving the IMSI.

2.3 IMS public identity

IMS public identities, which may perhaps be derived from the MSISDN, would have to be stored on the terminal as there is no storage location on the USIM. However, this is not considered to be a security problem.

2.4 Lack of storage on USIM for IMS security association

There are no dedicated files on the USIM for storing the IMS-specific integrity keys, cipher keys, key identifiers, key lifetimes, counter values, etc. (more generally the IMS security association). However, this only seems to limit the ability to move the USIM between different terminals without having to re-authenticate each time. Furthermore, GPRS can be accessed with non GPRS SIMs which do not have a dedicated file for storing the GPRS-specific Kc and CKSN.

2.5 Re-use of security functions for different purposes

It should be considered whether there are any security problems with using the same authentication key and algorithm in the USIM for both UMTS and IMS. A typical problem is that when the same key is used with two different algorithms in two different domains then compromise of one algorithm leads to vulnerabilities in both domains even if the other algorithm is robust. However, if we use the USIM for IMS security then, although the authentication key is the same for both IMS and UMTS authentication, it is always used with the same authentication and key agreement algorithms so the above-mentioned problem cannot occur. The derived cipher and integrity keys are used with different algorithms in UMTS and IMS, but the same cipher/integrity key set are never used for both UMTS and IMS because the authentication and key agreement protocol is run independently within each domain. Put simply: this is no different to GPRS where the same Ki/A3A8 is used with two different algorithms (A5 and GEA) for two different purposes (CS and PS connection security) and authentication is done separately for each domain.

3 Conclusion

A number of issues have been identified which impact whether or not it would be possible to use a R99 or Rel-4 USIM application for providing IMS security. SA3 are asked to verify the assumptions and conclusions made in this document.