3GPP TSG SA WG3 Security — S3#22 **S3-020029**

25 - 28 February 2002

Bristol, UK

3GPP TSG-CN1 Meeting #SIPadhoc0201 ***Tdoc N1-020155***

Phoenix, USA, 14. –18. January 2002

Title:	**Reply** Liaison Statement on Prevention of Identity Spoofing in IMS
Source:	CN1
To:	SA3
Cc:	SA2
Response to:	LS (N1-020004, S3-010673) on Prevention of Identity Spoofing in IMS from SA3

Contact Person:

Name:	Kevan Hobbis
Tel. Number:	+44 1628 765252
E-mail Address:	kevan.hobbis@hutchison3g,com

Attachments: None

1. Overall Description:

CN1 thanks SA3 for their liaison on Prevention of Identity Spoofing in IMS received as document N1-020004.

CN1 has considered the three solutions proposed by SA3 and has the following comments

1) The S-CSCF sends the integrity key IK and all public identities for which a user is registered (explicitly or implicitly) to the P-CSCF in message (SM3) 4xx Auth_Challenge of TS 33.203v070, section 7.2. Whenever the P-CSCF later checks the integrity of a SIP message from the UA, using integrity key IK, it checks that any IMPU in the SIP message is one of those received with IK in (SM3).
   There would be no need for the P-CSCF to know the private identity IMPI in this context.
   Please also note that it has not yet been specified how IK is carried in (SM3) , cf. the accompanying LS from S3#21 to CN1 in S3-010669. When addressing the issue raised in S3-010669 it could also be studied how the IMPUs could be included in (SM3).

CN1 Comments :

CN1 has agreed in principle how to transport CK and IK in SM3. Please see separate liaison response from CN1 where the details of that solution are discussed.

CN1 has agreed, at it's Cancun meeting in December 2001, that the P-CSCF will be informed of all implicitly registered public identities using the SUBSCRIBE/NOTIFY SIP methods. This is separate from the SM3 message flow.

2) When the P-CSCF verifies a SIP message from the UA using the integrity key IK it includes the IMPI which was received with IK in (SM3) before forwarding the message to the S-CSCF. The S-CSCF then checks that the IMPI corresponds to the IMPU in the received message.
   Note that currently there is no field to carry the IMPI in e.g INVITE messages. Note also that this assumes that the P-CSCF is able to retrieve the IMPI from message (SM3).

CN1 Comments :

CN1 agrees with the assessment of the status of this solution i.e. that the SIP enhancement to carry this data (IMPI) would need to be done.

From CN1 viewpoint Solutions 2 and 3 seem to be similar in requiring that the P-CSCF gets to know the IMPI. CN1 is already enhancing SIP to carry additional parameters and adding IMPI could be done as part of these enhancements. CN1 note that this solution has the advantage that the IMPI is not always sent over the radio interface as the P-CSCF inserts the correct IMPI associated with the verified IK as received in the REGISTER message.

3) The UA includes the IMPI in the protected part of any integrity protected SIP messages. The P-CSCF verifies the integrity of that message using IK and checks that the IMPI is the one which was received with IK in (SM3). The S-CSCF then checks that the IMPI corresponds to the IMPU in the received message. Note that currently there is no field to carry the IMPI in e.g INVITE messages.

CN1 Comments :

CN1 considers this to be very similar to solution 2, at least from the CN1 persepective.

<u>The CN1 conclusions are summarised below</u>

The CN1 preferred solution is the first alternative of echoing back all the explicitly and implicitly registered IMPUs in a separate NOTIFY message from the S-CSCF to P-CSCF so that P-CSCF could match the IMPU with the previously sent IK (and CK) at Registration time.

CN1 additionally notes that :-

> The P-CSCF has an association between IMPI and IK after the first registration. The P-CSCF will also have a list of all registered IMPU that are associated with this IMPI and IK. This data can be used to verify the integrity of subsequent messages. It is therefore not necessary to include IMPI in every INVITE request from the UE as the INVITE will be integrity checked.
>
> The very first REGISTER request must be authenticated. Later REGISTER messages can be integrity protected using IK. If the S-CSCF is aware of this protection, it could decide to REGISTER an IMPU without further authentication, depending on operator policy etc. However, authentication is mandated for REGISTER messages that are not integrity protected.

The second of these implies that the P-CSCF needs to indicate to the S-CSCF if a received REGISTER request was integrity protected or not. CN1 is studying how this may be done, and requests guidance on the information that the S-CSCF may require e.g. the IK used, how long it has been in use etc.

2. Actions:

To SA3 group.

ACTION : CN1 asks SA3 to consider the conclusions described above, and to inform CN1 if there are any issues that have been overlooked.

To SA3 group.

ACTION : CN1 asks SA3 to consider what information regarding the integrity protection of the REGISTER that the S-CSCF may require, and to inform CN1 of their conclusions.

3. Date of Next CN1 Meetings:

CN1_22	28th January – 1st February 2002	Sophia Antipolis, France
CN1_22bis	19th – 21st February 2002	Oulu, Finland