3GPP TSG SA WG3 #21bis NDS/MAP ad hoc **S3z020041**
Antwerp, Belgium
31st January – 1st February 2002

Source:	**SA3**
To:	**CN1**
Title:	**Registrations without user authentication and Identity Spoofing**
Contact:	**Adrian Escott** Email: adrian.escott@hutchison3g.com

Attached: N1-020155 (= S3-0202029) and N1-020004 (=S3-010673)

SA3 thanks CN1 for their liaison statement (S3-020029 = N1-020155).

SA3 accept CN1's proposal that sending all implicitly registered public identities to the P-CSCF solves the problem of protecting Identity Spoofing.

SA3 agrees that the ability to perform (re-) registrations without user authentication securely is a worthwhile enhancement for IMS.

SA3 have agreed that for registrations without user authentication, the S-CSCF needs to know that the REGISTER message was integrity protected. Currently it is believed that no other data is necessary at the S-CSCF to make the decision whether to authenticate or not.

In a previous liaison (N1-020004=S3-010673 attached), SA3 suggested two further methods that could be used to protect against Identify Spoofing.

Method 2 indicated that attaching the IMPI related to the security association to messages outside the registration procedure would be sufficient to protect against Identity Spoofing.

This analysis suggests that attaching data at the P-CSCF to messages from the UE that were integrity protected can solve the Identity Spoofing problem and enable (re-) registrations without user authentications. For each issue, different data may need to be attached.

In light of this SA3 wonder whether CN1 would like to re-consider the issue of passing the implicitly registered IMPUs down to the P-CSCF, particularly if it was only included to address the Identity Spoofing problem, in favour of allowing data to be attached to SIP messages to indicate information about the integrity applied by the UE to that message. If, however, the passing of implicitly registered IMPUs down to the P-CSCF is required also for purposes other than countering identity spoofing attacks then it would only be necessary in addition to attach data to REGISTER messages from the P-CSCF to the S-CSCF to indicate whether the message was integrity-protected or not.

Actions

CN1:

- To re-consider the issue of sending the implicitly registered IMPUs to the P-CSCF from the S-CSCF (if only included for security reasons) against the alternative of adding data to all messages to allow the S-CSCF to check the correct integrity was applied to all messages.
- To define a mechanism to carry the appropriate data (based on the above decision) between the P-CSCF and S-CSCF.
- Inform SA3 of any decisions made.

Date of Next SA3 Meetings:

SA3_22	25th – 28th February 2002	Bristol, UK
SA3_23	14th – 16th May 2002	Victoria Island, Canada

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.

The CN1 conclusions are summarised below

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

3GPP TSG SA WG3 Security — S3#21 **S3-010673**

27-30 November, 2001

Sophia Antipolis, France

From: **SA3**

To: **CN1, SA2**

Title: **Prevention of identity spoofing in the IMS**

Contact: **Guenther Horn**
Guenther.horn@mchp.siemens.de

Phone: +49 89 636 41494

1. Problem

Two contributions to SA3#21, S3-010633 (Dynamicsoft, Ericsson) and S3-010636 (Siemens), identified a problem with the current draft specifications for IMS security, TS 33.203 (S3), TS 23.228 (SA2), and TS 24.228 (CN1), which may lead to a fraudulent user setting up sessions under a false identity and consequently avoiding to be charged for the session. A more detailed description of the attack is included in S3-010633. The possible solutions of the problem involve assumptions about the use of identities for which SA3 requests guidance from CN1 and SA2.

The rest of section 1 gives background information regarding the source of the problem:

SIP messages between the UA and the P-CSCF are integrity protected. This integrity protection also provides message origin authentication. The authenticated origin may be identified by any identity to which the integrity key IK has been (explicitly or implicitly) bound in the registration procedure. These identities include the private identity (IMPI) and the registered public identities (IMPUs).

The S-CSCF needs to inform the P-CSCF about (a subset of) identities to be bound to IK when it sends IK in the registration procedure message (SM3) 4xx Auth_Challenge of TS 33.203v070, section 7.2. When the P-CSCF later verifies the integrity of a SIP message using a key IK it must (explicitly or implicitly) inform the S-CSCF about an identity bound to the IK used. E.g. the P-CSCF could be required to check the IMPUs bound to IK against any IMPU included in the received message. If no such a check is done, then a fraudulent user may e.g. use an IK bound to a registered IMPU of his to generate a correct message authentication code on an INVITE message, but include somebody else's IMPU in the INVITE message. This would lead to a number of threats, e.g. the S-CSCF would then charge the session to the false IMPU.

S3 has realised that simply adding a statement to the specifications that the P-CSCF always checks the IMPU bound to IK against any IMPU included in the received message is not sufficient. The main problem arises from the fact that IMPUs may be implicitly registered. But implicitly registered IMPUs are not known by the P-CSCF at registration time according to the current specifications; hence the P-CSCF cannot bind IK to those IMPUs. (Cf. also the LS from S3#21 to CN4 in S3-010668 where S3 informs CN4 that S3 sees a need to distribute implicitly registered IMPUs from the HSS to the S-CSCF.)

Any solution to the problem described in section 1 has to address two issues:

- which identities are bound to the integrity key IK in message (SM3) 4xx Auth_Challenge of TS 33.203v070, section 7.2?
- how does the P-CSCF inform the S-CSCF about an identity bound to the IK used to verify the integrity of a message received from the UA?

2. Possible solutions

S3 discussed various solutions and agreed to further study at least the following three possible solutions, and variants thereof:

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).

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).

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.

S3 is aware that other solutions are possible. However, solutions requiring additional round-trips have been ruled out. (This applies in particular to additional “end-to-middle” regular authentications for each INVITE mentioned as the third solution in S3-010633.) Also, S3 has ruled out solutions which would require two sets of user specific integrity keys, and/or integrity checks to be performed at two different IMS network entities. (This applies in particular to the creation of an additional session key mentioned as the fourth solution in S3-010633.)

3. Actions

CN1 and S2 are kindly asked to study solutions to the problem described in section 1 and comment on the three possible solutions mentioned in section 2. Other suggestions would be welcome, but should be checked by S3 from a security point of view.

4. **Attachments**

S3-010633, S3-010636, S3-010668, S3-010669