3GPP TSG CN Plenary Meeting #15 **NP-020034**
6th – 8th March 2002. Jeju, Korea.

Source: **MCC**

Title: **All LSs sent from CN1 since TSG CN#14 meeting,- pack 1**

Agenda item: **6.1.1**

Document for: **INFORMATION**

Introduction:

This document contains **6 agreed** LSs sent from **TSG CN WG1**, and are forwarded to TSG CN Plenary meeting #15 for information only.

Meeting	TDoc #	Status	Source	Tdoc Title	Type	Comments
N1-SIP0201	N1-020113	AGREED	Dynamicsoft/ Andrew Allen	(Required deletion of Sr interface)	LS OUT	
N1-SIP0201	N1-020127	AGREED	Ericsson / Miguel Garcia	Liaison Statement on Trace Activation Mechanism in SIP	LS OUT	Revision of N1-020104
N1-SIP0201	N1-020154	AGREED	Vodafone / Duncan Mills	IMS Security requirements and transportation of SIP session keys	LS OUT	Revision of N1-020103
N1-SIP0201	N1-020155	AGREED	Hutchison 3G / Kevan Hobbis	Prevention of identity spoofing in the IMS	LS OUT	Revision of N1-020105

Meeting	TDoc #	Status	Source	Tdoc Title	Type	Comments
N1-22bis	N1-020648	AGREED	Sofie	Liaison Statement on PSTN/CS domain originated call	LS OUT	Linked to 593. To:SA2 Cc:CN4
N1-22bis	N1-020665	AGREED	Kevan	Reply Liaison Statement on Registrations without user authentication and Identity Spoofing	LS OUT	To: SA3. Revised from 601

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-CN1 Meeting #22bis ***Tdoc N1-020665***
Oulu, Finland, 19. - 22. February 2002

Title: **Reply** Liaison Statement on Registrations without user authentication and Identity Spoofing
Source: CN1
To: SA3
Cc:
Response to: LS (N1-020597, S3-020041)

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

Attachments: None

---

1. Overall Description:

SA3 had three questions/points in their liaison. The responses are as follows.

- 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.

CN1 Reply :- This will be considered in the CN1 work. At this time CN1 has not concluded whether the sending of implicitly registered IMPU's to the P-CSCF can be deleted, and are still working on this and related issues.

- To define a mechanism to carry the appropriate data (based on the above decision) between the P-CSCF and S-CSCF.
-

CN1 Reply :- This is work in progress in CN1.

- Inform SA3 of any decisions made.

CN1 Reply :- CN1 agree to this.

CN1 have a related question for SA3 which is detailed below.

Question : Should the P-CSCF forward a REGISTER that includes an integrity check, but where the integrity check has failed, to the S-CSCF, or should it discard this REGISTER ?

2. Actions:

To SA3 group.

ACTION: CN1 asks SA3 opinion on the following question.

Should the P-CSCF forward a REGISTER that includes an integrity check, but where the integrity check has failed, to the S-CSCF, or should it discard this REGISTER.

3. Date of Next CN1 Meetings:

CN1_23	8th – 12th April 2002	USA
CN1_24	13th – 17th May 2002	Sophia Antipolis, France

3GPP TSG-CN1 Meeting #22bis ***Tdoc N1-020648***
Oulu, Finland, 19. - 22. February 2002

Title: Liaison Statement on PSTN/CS domain originated call
Source: CN1
To: SA2
Cc: CN4

Contact Person:
Name: Sophie Aveline
Tel. Number: +33 1 45 29 60 84
E-mail Address: sophie.aveline@francetelecom.com

Attachments:

---

1. Overall Description:

CN1, defining stage 3 specifications for IP Multimedia subsystem, discussed during the Oulu CN1#22bis meeting the routing, in IP Multimedia subsystem, of incoming call originated from PSTN/CS domain and reaching IMS through MGCF.
Such a procedure is described in TS 23.228 v5.3.0 in paragraphs 5.6.3 and 5.5 (in any sub-section of this section).

CN1 assumes the following cases may occur:

- IMS only subscription
- IMS/CS subscription
- CS only subscription
- No subscription

This Liaison Statement focuses on the case where the called user does not have IMS subscription but has CS subscription.

From SA2 specifications, CN1 understanding is the following one concerning the call signalling of PSTN/CS originated call routed towards MGCF:

- From PSTN/CS domain, a call can reach MGCF due to operator choice (no check is done on user subscription).
- MGCF initiates SIP INVITE request towards I-CSCF on reception of IAM message from PSTN/CS domain (the Request URI of the INVITE message is a TEL URL containing the E.164 number of the called user).
- I-CSCF queries the HSS for current location information.

At this step: What is the answer of the HSS to this query if the called user has no IMS subscription? (for instance CS only subscriber)
CN1 analysis is that to release the call is not the correct handling as the subscriber is a mobile user (even if he does not have IMS subscription).

Consequently, CN1 asks guidance to SA2 on the following question:
In such a configuration (ie PSTN/CS domain originated call reaching MGCF) how will the call be routed from MGCF to the user in the case he does not have IMS subscription?

2. Actions:

To SA2 group.

ACTION:

CN1 asks SA2 opinion on his understanding detailed in the following questions:

- Is there any check on user subscription done before a PSTN/CS domain originated call reaches MGCF?
  CN1 understanding: No
- Does the MGCF performs any check on user subscription or any DNS-ENUM query?
  CN1 understanding: No

- If the user does not have IMS subscription, result of query for location from I-CSCF to HSS will be the release of the call?

  CN1 understanding: Yes

In the case CN1 understanding is correct, CN1 asks SA2 guidance on the procedure when the called user of a PSTN/CS domain originated call reaching MGCF does not have IMS subscription.

3. Date of Next CN1 Meetings:

CN1_23	8th – 12th April 2002	USA
CN1_24	13th – 17th May 2002	Sophia Antipolis, France

3GPP TSG-CN1 Meeting #SIPadhoc0201 ***Tdoc N1-020154***

Phoenix, USA, 14. –18. January 2002

Title: Liaison Statement on transportation of SIP session keys from S-CSCF to P-CSCF

Source: CN1

To: SA3

Cc:

Response to: LS N1-012011 (S3-010669) on IMS Security requirements and transportation of SIP session keys from SA3

Contact Person:

Name: Duncan Mills

Tel. Number: +44 1635 676074

E-mail Address: duncan.mills@vf.vodafone.co.uk

Attachments: None

---

1. Overall Description:

CN1 thanks SA3 for the above liaison statement, and is pleased to respond.

SA3 highlighted the following three actions on CN1:

1. CN1 to inform SA3 whenever CN1 detects a security requirement is missing in TS33.203 before solutions are implemented in related CN1 Technical Specifications.
2. CN1 to remove the restriction on 3 re-authentication attempts.
3. CN1 to inform SA3 on how session keys are transported in SIP.

Firstly, with respect to action number 1, CN1 will certainly continue to review the stage two specification 33.203 and raise any issues that may arise with SA3.

Secondly, regarding action number 2, CN1 feels that the number of re-attempts to authenticate is something that greatly affects UE behaviour. It is important that a UE knows exactly what to expect from the network and exactly what to do if that expectancy is not met.

CN1 believes that for both aspects of mutual authentication failure (the UE continues to provide an incorrect RES or the network continues to provide an incorrect RAND+AUTN) the number of re-attempts should be limited.

For example, if the number of re-attempts is set by the operator, then the UE always has to expect and allow a further attempt (incorrect RAND+AUTN) or the UE is always allowed to retry a further time (when the network continues to provide challenges, even though the UE is sending incorrect RES). As far as the UE is concerned, the network has obviously decided to perform a very high number of re-attempts- as per the specification- and so the UE will continue to respond.

CN1 sees the above example as unacceptable, and prefers to follow the UMTS model and limit the number of re-attempts. This has the advantage of giving genuine UEs and genuine networks a further opportunity to authenticate correctly, in case the original failure was due to an error. It also means that after a pre-defined number of re-attempts, both the UE and the network can safely abort the procedure and assume 'foul play'.

The current number of re-attempts is specified as three. CN1 asks SA3 to decide whether or not they still require CN1 to alter this.

Finally, in response to action number 3, CN1 can report that it has agreed upon the following working assumption:

Session keys CK and IK will be passed from the S-CSCF to the P-CSCF in the EAP header of the 401 UNAUTHORISED response (along with the RAND and AUTN). The P-CSCF shall remove and store the CK and IK, before forwarding the 401 UNAUTHORISED response to the UE.

It is expected that detailed CRs will be agreed at the next CN1 meeting.

2. Actions:

To SA3 group.

ACTION: CN1 asks SA3 to reconsider specifying the number of authentication re-attempts as being an operator choice.

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-CN1 Meeting #SIPadhoc0201 ***Tdoc N1-020127***

Phoenix, USA, 14. –18. January 2002

Title: Reply to Liaison Statement on Trace Activation Mechanism in SIP

Source: CN1

To: SA5 SWG_B (RG Tracing)

Cc: CN4

Response to: S5-010749

Contact Person:

Name: Miguel A. Garcia

Tel. Number: +358 40 514 0002

E-mail Address: miguel.a.garcia@ericsson.com

Attachments: N1-020003

---

1. Overall Description:

CN1 thanks SA5 for the Liason Statement S5-010749 (N1-020003, attached) on Trace Activation Mechanism in SIP.

CN1 would like to understand the motivation and need for such a mechanism within IMS.

For a user that is already registered, all the SIP signalling originated by the UE or terminated by the UE is traversing the allocated S-CSCF in the home network, via a given P-CSCF and possibly the I-CSCF. This procedure is the same irrespective of whether the user is roaming or not. As a consequence, the S-CSCF is already receiving a very detailed trace of all the signalling originated or terminated by the UE. Whatever information is available at the P-CSCF is already available at the S-CSCF. Note that these mechanisms are significantly different from the GSM procedures.

For a user that is not registered, there is not a S-CSCF allocated in the home network because the S-CSCF is dynamically allocated at registration time. The user is not able to send any other signalling that SIP REGISTER messages and is not able to receive any other signalling than responses to the SIP REGISTER messages.

CN1 believes that as all the SIP signalling is always traversing the S-CSCF in the home network, the S-CSCF is already well informed on the SIP activities originated or terminated by the user. Therefore, at their current level of understanding of this issue, CN1 believes that the trace activation mechanism may be triggered by the HSS towards the S-CSCF through the Cx interface. This mechanism does not involve the P-CSCF.

More detailed information on call flows and the parameters that are available by the S-CSCF can be found in 3GPP TS 24.228

CN1 has not been able to understand the real requirements for the proposed solution. CN1 would like to understand those requirements isolated from a possible technical implementation or solution.

2. Actions:

To SA5 group.

ACTION:

CN1 kindly requests SA5 to study the information provided above, together with the call flows in 3GPP TS 24.228. CN1 also request SA5 to reconsider the requirement for trace activation one more time together with the information described above.

If SA5 considers that the requirements are still valid, CN1 would like to hear and understand what are those requirements and keep them separated from a possible solution to solve the problem.

SA5 should also consider the required timescales. CN1 has to complete work on its specifications at their February meeting.
Finally, in case the proposed solution to activate the trace (the HSS activates the trace to the S-CSCF) is acceptable for SA5, CN1 suggests SA5 to contact CN4 that is responsible for the developing of the Cx interface.

3. Date of Next CN1 Meetings:

Meeting	Date	Location	Host
CN1 #22	**28 Jan - 01 Feb 2002**	**Sophia Antipolis, France**	**ETSI**
CN1 #22bis	**19 - 22 Feb 2002**	**Oulu, Finland**	**Nokia**
CN1 #23	**8 - 12 April 2002**		

4. Attachments:

N1-020003_LS IN.zip

3GPP TSG-CN1 SIP Adhoc Meeting 0102 ***Tdoc N1-0201113***

Phoenix, USA, 14-18. January 2002

Title: **LS on Sr interface between Application Server and MRFC**

Source: **TSG CN WG1**

To: **TSG SA WG2**

cc: **TSG CN WG1, TSG CN WG4**

Date: **15 January 2002**

Contact Person:
Name: **Andrew Allen**
Company **dynamicsoft**
E-mail Address: **aallen@dynamicsoft.com**
Tel. Number: **+1 972 473 5507**

---

1. Overall Description:

Currently TS 23.228 defines the Sr interface between the Application Server (AS) and the MRFC in addition to the Mr interface between the S-CSCF and the MRFC. However currently TS 23.228 does not define any further detail as to the required functional behaviour on the Sr interface.

TSG CN WG1 is currently working towards completion of the IMS Technical Specifications for Rel 5 by March 2002 and would like to inform TSG SA WG2 that no contributions have been received to date within TSG CN WG1 proposing a suitable protocol to be used on the Sr interface.

Given that there are only two additional TSG CN WG1 meetings before the expected presentation of the IMS Technical Specifications to TSG CN#15 for approval in March 2002 TSG CN WG1 believes it is unrealistic to expect completion of any stage 3 specification work on the Sr interface within the Rel 5 timeframe. TSG CN WG1 would therefore like to inform TSG SA WG2 that it intends to delete any reference to and support for the Sr interface within the IMS Specifications TS 23.218, TS 24.228 and TS 24.229.

2. Actions:

TSG SA WG2 is requested to align the IMS stage 2 with the stage 3 by removing the Sr interface from the Rel 5 versions of TS 23.228.

3. Date of Next TSG CN WG1 Meetings:

CN1 #22	28 Jan. – 1 Feb 2002	Sophia Antipolis, France.
CN1#22Bis	19Feb - 22 Feb 2002	Oulu, Finland