3GPP TSG-CN1 Meeting #31 ***Tdoc N1-031199***
Sophia Antipolis, France, 24-29 August

Title: Liason statement on Profiling of RFC3325 for IMS
Response to: N1-030994
Release: REL-6

Source: CN1
To: SA3
Cc: SA1, SA2

Contact Person:
Name: Gábor Bajkó
Tel. Number: tel:+36 20 9849259
E-mail Address: Gabor.Bajko@nokia.com

Attachments: None

1. Overall Description:

CN1 thanks SA3 for the liaison statement regarding the Profiling of RFC3325 for IMS requirements for Rel-6.

CN1 has briefly discussed the LS and other related CN1 CRs relating to IMS openness and the trust domain concept, and the following conclusions were made:

Currently there are no requirements in 3GPP that the home IMS network must have the knowledge whether the destination network is IMS network (and therefore trusted) or not.
CN1 has procedures to determine whether the next hop SIP Proxy is part of the same domain or another domain. The discussion about the removal of the P-Asserted-Identity header (if privacy id was requested by the user) was postponed until 3GPP can reach a conclusion on the requirements relating to the knowledge of the trustworthiness of the destination network. If a solution is developed for this information to be available in the home network, the P-Asserted-Identity header field will not need to be removed by the home network, rather by the destination network (if privacy id was requested). If a solution is not found to the problem above, the P-Asserted-Identity header will need to be removed in the home network.
CN1 can confirm that from RFC3325 only the privacy none and privacy id options were included into Rel5, the other privacy options were left for Rel6 because they require additional procedures for the CSCFs. CN1 believes that from security architecture point of view there is no difference between the handling of the different user privacy options, they all require some information removal from SIP headers.

CN1 has agreed to a CR listing procedures for the I-CSCF regarding SIP messages received from non-trusted domains. The procedures require the I-CSCF to know whether the message has been received from a trusted domain or not. This probably narrows down the possibilities listed in bullet 4 of Spec(T), but CN1 has no strong preference on which solution to be adopted. It should be mentioned that for Rel6 IMS, CN1 does not plan to have different CSCFs for access to/from Internet and/or other non-trusted domains.

CN1 does not understand the problem statement in bullet 5 and 8 of Spec(T). CN1 has already got procedures for handling id privacy in IMS.
At the edge of IMS the P-CSCF inserts a P-Asserted-Identity header into the requests/responses, and that identity will be trusted by all entities within the trust domain, including applications servers hosting different services like Presence, Conferencing, etc.

CN1 has always assumed that Rel-5 IMS network is a closed network, i.e. messages will not be sent outside IMS and will not be received from outside IMS. Therefore, Rel-5 24.229 does not have any procedures describing what actions the CSCFs shall perform when such scenarios are faced. Such procedures are planned to be defined for the Rel-6 version of 24.229.

CN1 would like to draw the attention of SA3 that anonymity is only a subset of privacy, referring in most cases to media anonymity i.e hiding the IP address of the party which requested it. In order to provide this, a middlebox (anonymiser) is required in the architecture. Such middlebox currently does not exist in the architecture; therefore IP address hiding is currently not supported. S3-030377 uses the terms ‘anonymity’ and ‘privacy’ interchangeably, which may lead to confusions.

2. Actions:

To SA3 group.

ACTION: SA3 is asked to take into consideration the analysis made above.

3. Date of Next TSG-CN1 Meetings:

CN1_27	27st – 31st November 2003	Bangkok, Thailand