**3GPP TSG SA WG3 Security — S3#25** **S3-020480**
**8 - 11 October 2002**
**Munich, Germany**

---

**3GPP TSG-CN1 Meeting #26** ***Tdoc N1-022160***
**Miami Beach, Florida, USA, 23 – 27 September 2002**

| | |
|---|---|
| **Title:** | Liaison statement on Interoperability Issues and SIP in IMS |
| **Response to:** | LS N1-021962 (NP-020393) and LS N1-022045 (SP-020627) on Liaison Statement on Interoperability Issues and SIP in IMS |
| **Release:** | Release 5 |
| **Work Item:** | IMS-CCR |
| | |
| **Source:** | CN1 |
| **To:** | SA1, SA2, SA3, CN, SA |
| **Cc:** | SA4, SA5, CN2,CN3, CN4,CN5 |


**Contact Persons:**

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

**Name:** Krisztian Kiss
**Company:** Nokia Corporation
**Tel. Number:** +358 50 4835363
**E-mail Address:** krisztian.kiss@nokia.com


**Attachments:** None

---

**1. Overall Description:**

CN1 thanks TSG SA for their Liaison statement on Interoperability Issues and SIP in IMS.

CN1 have completed a preliminary analysis of the specific technical issues identified by IETF Working Group Chairs, Area Directors, and IESG members in the Liaison to 3GPP and would like to inform other 3GPP working groups of the outcome of this analysis.

The CN1 analysis of the specific technical issues is below:

## 1) The P-CSCF initiating BYE requests

*"The P-CSCF may send a BYE on behalf of the UA, generally because the P-CSCF has been notified by the radio layer that the UA has lost contact. Of course, the P-CSCF doesn't have the credentials to provide authentication of the BYE, so many UAs will consider this to be a forged message. This also renders 3GPP UAs vulnerable to denial of service attacks using forged BYEs."*

This issue has been previously identified by CN1 and the solution that addresses forged BYEs from 3GPP terminals has been implemented based on the P-CSCF verifying that all BYEs comes from the same terminal that created the dialog. This does not prevent the possibility of forged BYEs originating from external networks such as the Internet if the dialog parameters were snooped. CN1 believes this remaining issue is an Internet interoperability issue to be resolved in release 6.

CN1 has identified that this issue arises from SA2 architectural requirement in Clause 5.10.3.1.2 "P-CSCF initiated session release after loss of radio coverage" [TS 23.228 v5.5.0].

**CONCLUSION:**
**The current implementation is seen by CN1 as the currently agreeable technical solution within the existing SIP RFCs based on these requirements. CN1 believes that it is not possible to resolve this issue in release 5 unless the requirement changes.**

## 2) The P-CSCF stripping headers

"*The P-CSCF strips away Route, Record-Route, Via, Path, and Service-Route headers before passing messages on to the UA. It then reinserts them messages in the other direction, and may also strip out Route headers inserted by the UA. This breaks end-to-end protection using S/MIME and prevents the UA from accessing external services using loose routing. It also prevents the UA from knowing about any proxies that may have piggybacked on its registration using the Path mechanism, which is a serious violation of the openness principle and leaves 3GPP users registering with external servers subject to certain man-in-the-middle attacks affecting REGISTER messages without any way to detect those attacks."*

Header stripping by the P-CSCF is primarily intended to protect the network from malicious UEs that could try to bypass some IMS network elements (e.g. the S-CSCF). The IMS network ensures that the UE has no means to skip certain elements from Record-Route, Via or Service-Route header fields when creating the corresponding Route or Via header fields, as that would result in a situation that UEs could bypass for instance the S-CSCF by omitting it from the Route and/or Via header and charging of the user might be bypassed.

CN1 believes that the man-in-the-middle attack should not be an issue in 3GPP where network domain security (hop-by-hop IPSec integrity protection) is deployed between all nodes.

CN1 believes that header stripping does not affect the UE compliancy with the routing procedures described in RFC3261, however Path and Service-Route extensions are not required to be implemented by the UE.

Regarding the UE, CN1 has discussed a contribution that attempts to mandate the UE to implement the Path and Service-Route extensions in order for the UE to be compliant with IETF procedures. However the current P-CSCF behaviour regarding routing and header stripping will not change. Some companies believe that this preserves possibilities for future solutions in release 6. However this has not yet been accepted in CN1 and requires further analysis on the full impacts on IMS nodes and would not resolve this problem in release 5 and would maintain header stripping.

Registration with external registrars can be performed without involving IMS but rather as a regular PS domain service.

However in addition to the issues identified by IETF CN1 has also identified that there maybe future issues with supporting any future new SIP mechanisms that create complex SIP dialogs that are not understood by the P-CSCF and this may hinder new service creation.

There are varying opinions about the importance of this when operating CSCFs of different releases and different networks

CN1 also considers the requirements for IMS node address security and hiding and also reducing the size of messages sent over the air interface (although potentially reduced by use of SIP compression) to be relevant in the solution currently agreed by CN1.

CN1 has identified that the current solution arises from the SA1 requirement “It shall be possible to limit the view of an operator’s network topology to authorised entities. “ [TS 22.228 V5.6.0] and the SA2 architectural requirements in TS 23.228 regarding home control of services and the basic SA2 information flows.

CN1 will consider allowing for the UE to perform loose routing by inserting Route header values to initial requests. These Route headers would then be used by the UE's S-CSCF to route the originating initial requests accordingly. It has yet to be determined by CN1 if this can be incorporated in release 5 or release 6.

**CONCLUSION:**
**The current implementation is seen by CN1 as the currently agreeable technical solution based on all these requirements. CN1 believes that it is not possible to completely resolve this issue in release 5 unless the basic requirements change.**

## 3) CSCFs editing SDP

"*The CSCF may edit SDP sent from or to the UA in order to force the selection of codecs considered favorable to the operator. This has the side effect of breaking end-to-end protection of the SDP using S/MIME. It also precludes interoperating with external elements when both the IMS UA and the external UA share only a common codec not supported by the P-CSCF."*

CN1 identified that it is an operator requirement that the operator must have the ability to ensure that the UE requested media components and/or codecs comply with those authorised for the subscriber both in the visited network (based on local operator policy) and in home network (based on local operator policy and subscriber profile).

The IMS codec negotiation is completely based on the SIP/SDP offer/answer model. The offer/answer model is fundamentally of end-to-end nature, as it is driven by end-user preferences and terminal capabilities.

The SIP compliant way to perform any such SDP modifications requires a B2BUA. B2BUAs cause some of the side effects identified by IETF and also are less performance efficient than pure SIP proxies and can break Signaling Transparency. CN1 has identified no current interoperability issues but this might cause future interoperability issues if IETF extends SDP.

Potential alternative solutions have been discussed in IETF but have not progressed and these could not be available for release 5. Such alternative solutions would also require a change to the SA2 architectural requirements in TS 23.228 clause 5.11.3.1 that is very specific as to how the service requirement should be implemented by CN1.

CN1 has identified that this issue arises from SA1 requirement “Possibility for a network operator to implement IP Policy Control for IP multimedia applications.” and “In order to support the user's preferences for IP multimedia applications, the capability negotiation shall take into account the information in the user profile whenever applicable. “[ TS 22.228 V5.6.0] and SA2 architectural requirement among others in TS 23.228 clause 5.11.3.1 “Codec and media characteristics flow negotiation during initial session establishment.”

**CONCLUSION:**
**The current implementation is seen by CN1 as the current agreeable technical solution based on these requirements. CN1 believes that it is not possible to resolve this issue unless the requirement changes.**

## 4) S-CSCF obfuscating To: and From: fields

*"The S-CSCF MAY (we believe this is still being discussed in 3GPP) obfuscate the To: and From: fields in messages. This appear to be based on a particular interpretation of privacy regulation in certain European domains. It has the side effect of breaking end-to-end protection with S/MIME and breaking external services using the To: and From: fields, such as the most common forms of caller-ID used with SIP today."*

**CONCLUSION:**
**There is currently only a configuration option to obfuscate the From header based on Operator Policy. CN1 is considering the possibility in release 5 of removing this possibility completely and having a clear statement that From headers should not contain privacy revealing information when the user requires Privacy.**

## 5) P-CSCF performing identity checks

*"The P-CSCF filters messages from the UA to assure that only an identity known to the P-CSCF is presented by the UA. This may interact with the preceding characteristic. This appears to be required to accommodate the authorization model of 3GPP, which authenticates only REGISTER transactions and uses them to establish a security association between a UA and the P-CSCF. The side effect is that a 3GPP user may use only the operator-provided identity and may not be able to effectively use third-party services that provide other identities unless those services provide identity transformation with a back-to-back user agent."*

The procedure how IMS networks validate and assert users’ identities follows draft-ietf-sip-asserted-identity. It is the understanding of CN1 that the current procedures comply with IETF SIP. It is understood by CN1 to be a SA1 requirement that the IMS operator needs to be aware of the identity used in any SIP request. What is authenticated is the P-Asserted-Identity header so the third-party application could use another identity contained in the From header. These are not authenticated and so the third-party services should still be able to

supply an identity configured by the user compliant with basic SIP in RFC 3261 and using the IMS operator supplied identity which is authenticated to reach the third party service supplier via the IMS.

CN1 has identified that the current solution arises from SA1 requirement “Public identities shall be administered by the network operator and shall not be changeable by the user. It shall be possible for the network operator to guarantee the authenticity of a public identity presented for an incoming call to a user where the call is wholly within that operator’s network (i.e. originating and terminating parties are subscribers to, and resident in, a single PLMN). “ And “The IM CN subsystem shall be able to verify at any time that the user is entitled to use the resources of the IM CN subsystem”. [TS 22.228 V5.6.0] and the SA3 IMS security architecture in TS 33.203.

**CONCLUSION:**
**CN1 believes that this is not an issue and does not plan on any changes unless the security requirements should change.**

## 6) Network configuration hiding

*"The I-CSCF (or THIG) may encrypt Via and Route information when acting in topology-hiding mode. This was allowed for in earlier SIP specifications, but the use has been deprecated for a variety of reasons. The exact impact on interoperability remains unknown."*

The possibility to optionally provide topology hiding of the network nodes in one IMS network from another IMS network is an operator requirement from stage-1 and stage 2 specifications. The mechanism adopted by CN1 is not supported by RFC 3261 or any other RFC but CN1 has identified no current interoperability issues.
CN1 has identified that this issue arises from SA1 requirement ““It shall be possible to limit the view of an operator’s network topology to authorised entities. “ [ TS 22.228 V5.6.0] and the SA2 architectural requirements in TS 23.228.

**CONCLUSION:**
**The current implementation is seen by CN1 as the currently agreeable technical solution based on these requirements. CN1 believes that it is not possible to resolve this issue unless the requirement changes.**

## 7) CSCFs manipulating message bodies

*"Some CSCF elements and AS may manipulate message bodies. Manipulating message bodies in a proxy is forbidden in RFC 3261 because it breaks end-to-end protection using S/MIME. These elements do not appear to implement all of the UA behavior that would enable them to preserve end-to-end protections."*

The concept of carrying IMS intra-system information in XML bodies of SIP messages has been mainly superseded by SIP Private extensions (P-headers). All the 3GPP P-headers are documented as a single IETF I-D. Otherwise the issue is the same as for 3).

The remaining XML body is for the S-CSCF inserting Service-Info XML body into message bodies. TS 23.218 is open ended but currently TS 24.229 only allows this for the third-party REGISTER to the AS where S-CSCF acts as a UA which means it does not violate RFC 3261. No need has been identified for this to be used in any other request other than the REGISTER.

**CONCLUSION:**
**CN1 is currently discussing tightening up the 23.218 text restricting use of Service-Info to third-party REGISTER. This could be done by CN1 in release 5.**

**2. Actions To SA1, SA2, SA3:**

CN1 requests SA1, SA2, and SA3 to take into account the analysis above in responding to the SA liaison. CN1 also requests SA1, SA2 and SA3 to inform CN1 about the necessary actions needed to be taken by CN1 based on their discussions.

**3. Date of Next TSG-CN1 Meetings:**

| | | |
|---|---|---|
| CN1_27 | 11th – 15th November 2002 | Bangkok, Thailand |