

Title: [DRAFT] Liaison statement on Interoperability Issues and SIP in IMS

Source: TSG CN

To: TSG SA

Cc:

Release: Release 5

Work Item: IMS-CCR

Agenda item:

Document for: INFORMATION

Contact Persons:

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

Attachments: None

1. Overall Description:

At CN#18, progress was made in the area of addressing the concerns raised by the IETF on SIP interoperability. In particular, the following CRs were approved:

- o NP-020663 and NP-020555 (CR 073) – Issue 2 (The P-CSCF Stripping Headers): conditional on SA approval of corresponding 23.228 CR
- o NP-020668 – Issue 3 (CSCFs editing SDP): conditional on SA approval of corresponding 23.228 CR
- o NP-020561 (CR 247) and NP-020564 (CR 282) – Issue 4 (S-CSCF obfuscating To: and From: fields)
- o NP-020552 (CR 038) – Issue 7 (CSCFs manipulating message bodies)

A draft liaison towards IETF is provided below. This describes the progress that has been made in addressing these issues with options A and B for issue 3.

Option A corresponds to the SDP editing solution, which is currently implemented in the Release 5 specifications.

Option B corresponds to the new proposal, which is based upon SDP negotiation using an error message to indicate the availability of codecs to the UE.

These represent the controversial pending SA decision on SDP editing. If SA approves the company contribution on “Handling of SDP manipulation issue in stage-2 specifications” (SP-020675) then Option B text should be used. Otherwise Option A text will be maintained.

This draft liaison provides analysis and describes in detail the current resolution of each of the items raised by IETF. It assumes that SA will approve all the related SA2 working group agreed CRs against TS 23.228 on these issues. SA is encouraged to use this text as a baseline for responding to the IETF.

CN proposes as a next step for release 6 that a joint 3GPP-IETF workshop be organised with participation by members of CN1, SA1, SA2 and SA3 during February 2003 to resolve those issues that remain in release 5 and those that arise for release 6. CN requests SA to encourage active participation by members of its working groups in such a meeting.

In addition, the following issues were raised during the CN discussions regarding SDP media authorisation, which SA should be aware of:

1. Risk of having no suitable codec among involved networks:

For both options A and B there is a possibility that different network policies for supported codecs could lead to a situation where no suitable codec is available; the call cannot therefore be supported and must be rejected. For Option A, this failure can be determined quickly however in this case the calling party would be unaware of why the session establishment failed and unaware that an alternative codec selection may be successful. For Option B this may take several repeat requests and therefore take considerable time however there is the possibility for the network to suggest an alternative codec. The solution to this is not to adopt a more efficient solution, but to reduce the number of session requests that will fail due to policy control.

CN therefore asks SA to develop guidelines to network operators concerning policy control, such that network operators adopt more common policy control practices. There may also be material appropriate to the user equipment, concerning what codec sets should be requested in the first place.

2. Session Set-up Delay

With Option B (using the 488 error message) then there is the possibility that in some cases there could be multiple signalling exchanges (maximum of four cycles) between the UE and different CSCF nodes, which would significantly slow down the session establishment. Some operators have identified this as an issue of concern. If SA chooses Option B, solutions need to be considered to minimise this possibility.

3. Minimising Possibility of Set-up Delay for Successive Sessions establishment attempts (Using Option B)

In order to avoid multiple reattempt scenarios during successive session set-up, consideration should be given to establishing mechanisms that cache information in either the network or UE regarding available codecs. CN therefore ask SA, if Option B is chosen, to develop the appropriate guidelines for a solution to this.

4. Error handling in the case that UE violates procedures

There was a concern that using Option B that there is a need for network based error-handling solutions in the case that the UE keeps retrying the same unacceptable request. If SA chooses Option B then solutions should be developed to handle this possibility appropriately.

2. Actions To TSG SA:

1. SA is requested to initiate work to develop common policy control practices and solutions that maximise effective session establishment.
2. SA is requested to send a response to IETF based on the text provided below with the appropriate Option A or Option B based on the SA decisions.
3. SA is requested to encourage active participation by members of its working groups in a joint 3GPP-IETF workshop.

3. Date of Next TSG-CN Meetings:

CN1_19

12th – 14th March 2003

Birmingham UK

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

~~Following their preliminary analysis of the specific technical issues identified by IETF Working Group Chairs, Area Directors, and IESG members in the Liaison to 3GPP CN1 has held a joint meeting with SA2 on these issues. As a result of the outcome of the discussions at the joint meeting with SA2 and additional discussion on CRs at CN1#27, CN1 has been able to make additional progress on addressing. The updated information on the progress in release 5 for each of the specific technical issues is indicated below with revision marks over the preliminary analysis documented in N1-022160:~~

3GPP has completed a detailed technical analysis of the technical issues identified by the IETF working group chairs in their liaison statement. This analysis included a joint meeting between the 3GPP system architecture group (SA2) and the Service Requirements group (SA1) and also another joint meeting between SA2 and the group working on the SIP protocol details (CN1). In addition the security group (SA3) has also analysed the security related aspects. As a result of these discussions the existing 3GPP service requirements were reaffirmed and a number of changes were made to 3GPP release 5 IMS specifications to address some of these issues. However some issues still remain and will need further work between 3GPP and IETF to resolve in 3GPP release 6.

3GPP proposes that a joint workshop be organised during February 2003 between 3GPP and IETF to resolve those issues that remain in release 5 and those that arise for release 6 while still meeting the 3GPP service requirements.

The detailed analysis of the issues and the identified solutions that follows is a composite of the analysis completed by the 3GPP working groups and is provided for the benefit of IETF SIP experts.

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."

3GPP requires the ability to terminate an ongoing session from the network, i.e. CSCF nodes. This is essential for charging and policy functions for IMS in 3GPP.

This issue has been previously identified by ~~CN1-3GPP~~ 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. ~~CN1-3GPP~~ believes this ~~remaining~~ issue is an Internet interoperability issue to be resolved in release 6.

3GPP observe another scenario when a SIP User Agent outside of IMS would like to authenticate BYE request from IMS P-CSCF. In this case, the external User Agent is a valid one instead of an attacker. 3GPP agree that a forged BYE from an external network is an Internet interoperability issue as well to be resolved in release 6.

~~CN1 has identified that~~ this issue arises from ~~SA2-the~~ 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 ~~CN1-3GPP~~ as the currently agreeable technical solution within the existing SIP RFCs based on these requirements. As there are no alternative approaches currently identified, ~~CN1-3GPP~~ 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~~ was 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 needs to 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.

CN1-3GPP 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 CN1-3GPP has also identified that there maybe future issues due to the call stateful behaviour of the P-CSCF 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 within 3GPP about the importance of this when operating CSCFs of different releases and different networks

CN1-3GPP 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 have been relevant in the solution currently previously agreed ~~by CN1~~.

CN1-3GPP 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:

Following joint discussions ~~with SA2 between the protocol and architecture working groups and the agreement of SA2 to CRs against TS 23.228~~ CN1-3GPP has agreed changes in release 5 to TS 23.228 and TS 24.229 in CR-073. This CR replaces the P-CSCF stripping of headers mechanisms with the UE-P-CSCF matching and enforcing the headers required by the Service Route, Via and Record Route procedures in order to avoid the possibility of bypassing the charging mechanisms. This CR-change also mandates the support of the Path, Service-Route and RFC 3261 routing mechanisms in the release 5 3GPP UE.

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."

[CN1-3GPP](#) has 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. [CN1-3GPP](#) 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-the](#) 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~~.

[CN1-3GPP](#) has identified that this issue arises from [SA1-service](#) 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-the](#) architectural requirement among others in TS 23.228 clause 5.11.3.1 "Codec and media characteristics flow negotiation during initial session establishment."

[The usage of S/MIME from UA to UA mentioned would sacrifice current 3GPP service requirements. When tunnelling SIP messages inside S/MIME, requirements pointed out in issue 2 would be prohibited as well. An alternative may be investigated whether S/MIME usage could be exercised between one 3GPP network element and a SIP User Agent outside of IMS. However, 3GPP do not believe that such an investigation could be concluded in Release 5.](#)

CONCLUSION:

[OPTION A:](#)

The current implementation is seen by [CN1-3GPP](#) 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.~~

[OPTION B:](#)

[CN1-3GPP](#) has ~~discussed possible~~[agreed](#) changes in release 5 to TS 24.229 ~~and to TS 23.228 in CR-284~~. This ~~CR-change~~ replaces the P-CSCF and S-CSCF mechanisms for editing the SDP for the purposes of authorization of media parameters. This CR instead enables CSCF rejection of requests that contain SDP that does not conform to the relevant policies. Rejection is achieved using a 488 (Unacceptable Here) response that contains SDP indicating SDP parameters that would be acceptable. ~~This CR has been technically reviewed by CN1 but could not be approved due to the fact that the related TS 23.228 CR has not been approved and objections to some of the technical details by a single company and reservations by another company about agreeing the solution before further evaluation.~~ This change ~~would~~[does](#) not completely address all the B2BUA issues associated with what ~~is~~[the previous procedures](#) in TS 24.229. It is also possible that in release 5 IMS non standardised solutions to transcoding, NAT and firewall transversal may also cause some minimal modification of SDP.

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 was only a configuration option to obfuscate the From header based on Operator Policy. [CN1-3GPP](#) has agreed ~~CR-246-rev-2 and CR-282~~[changes](#) against TS 24.229 in release 5, which removes this possibility completely and has a clear statement that From headers should not contain privacy revealing information. [3GPP now considers this issue resolved.](#)

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 RFC 3325](#). It is the understanding of [CN1-3GPP](#) that the current procedures comply with IETF SIP. It is understood by [CN1-3GPP](#) to be a [SA1-service](#) 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.

[CN1-3GPP](#) has identified that the current solution arises from [SA1-the service](#) 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.

[No attempt has been made within 3GPP to change security requirements for IMS. It is seen as essential that operator's network must be able to verify the identity has an association with the subscription ID to be charged, and the association should be established before usage. This however, does not impose restriction to services provided by any third party.](#)

CONCLUSION:

[CN1-3GPP](#) 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 [CN1-3GPP](#) is not supported by RFC 3261 or any other RFC but CN1 has identified no current interoperability issues. [CN1-3GPP](#) has identified that this issue arises from [SA1-the service](#) 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.

[This issue has been discussed and it was clarified in TS 23.228 that it is an operator's choice if they want such implementation in their IMS networks and 3GPP specifications provide the solution on how to achieve this.](#)

CONCLUSION:

The current implementation is seen by [CN1-3GPP](#) as the currently agreeable technical solution [for this optional requirement](#) ~~based on these requirements.~~

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~~ was 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:

CN1-3GPP has agreed a ~~CR-038~~ change to TS 23.218 that tightens up the TS 23.218 text restricting use of Service-Info to third-party REGISTER in release 5.