3GPP TSG CN Plenary Meeting #19 **NP-030011**
12th - 14th March 2003. Birmingham, U.K.

Title: **Response to IETF Concerns on SIP and IMS Interoperability**

Source: **3GPP TSG SA**

Agenda item: **5.2**

Document for: **INFORMATION**

Technical Specification Group Services and System Aspects **TSGS#18(02)0842**
Meeting #18, New Orleans, USA, 9-12 December 2002

To: **IETF**
CC: **3GPP TSG CN**

Release: **Release 5**

Work Item: **IMS-CCR**

Agenda item:

Document for: **INFORMATION**

Contact Persons:
Name: Stephen Hayes
Tel. Number: +1 469 360 8500
E-mail Address: stephen.hayes@ericsson.com

Attachments: None

---

1. Overall Description:

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 the end of January 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.

<u>1) The P-CSCF initiating BYE requests</u>

"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 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. 3GPP believes this 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.

This issue arises from 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 3GPP as the currently agreeable technical solution within the existing SIP RFCs based on these requirements. As there are no alternative approaches currently identified, 3GPP believes that it is not possible to resolve this issue in release 5.

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 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 ensure 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.

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.

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 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

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 previously agreed.

3GPP has identified that the solution arises from the architectural requirements in TS 23.228 regarding home control of services and the basic information flows.

CONCLUSION:

Following joint discussions between the protocol and architecture working groups 3GPP has agreed changes in release 5 to TS 23.228 and TS 24.229. This replaces the P-CSCF stripping of headers mechanisms with the 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 change also mandates the support of the Path, Service-Route and RFC 3261 routing mechanisms in the release 5 3GPP UE.

<u>3) CSCFs editing SDP</u>

"*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."*

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. 3GPP 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 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.

3GPP has identified that this issue arises from 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 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:
3GPP has agreed changes in release 5 to TS 24.229 and to TS 23.228. This 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 change does not completely address all the B2BUA issues associated with what 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.

<u>4) S-CSCF obfuscating To: and From: fields</u>

"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. 3GPP has agreed 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.

<u>5) P-CSCF performing identity checks</u>

"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 RFC 3325. It is the understanding of 3GPP that the current procedures comply with IETF SIP. It is understood by 3GPP to be a 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.
3GPP has identified that the current solution arises from 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 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:
3GPP believes that this is not an issue and does not plan on any changes.

<u>6) Network configuration hiding</u>

"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 3GPP is not supported by RFC 3261 or any other RFC but CN1 has identified no current interoperability issues.
3GPP has identified that this issue arises from 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 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. No Changes are required to TS 24.229.

CONCLUSION:
The current implementation is seen by 3GPP as the currently agreeable technical solution for this optional requirement.

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 was open ended but 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:
3GPP has agreed a 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.

2. Actions To IETF:

1. Please note the discussion and resolution of each of the interoperability issues raised by the IETF WG chairs.
2. Participation by SIP/SDP experts in the planned IETF/3GPP workshop is requested to address outstanding interoperability issues for Release 6.

3. Date of Next TSG-SA Meetings:

CN#19	17^{th} – 20^{th} March 2003	Birmingham UK